<理學碩士學位論文>

크랙정보 수집 프로그램 활용한 지적재산권 침해 사범 수사의 위법성 여부

Illegality of Investigation using the Crack-Information Gathering Program on infringement of the intellectual property rights

2016. 12.

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공

김 지 아

크랙정보 수집 프로그램 활용한 지적재산권 침해 사범 수사의 위법성 여부

Illegality of Investigation using the Crack-Information Gathering Program on infringement of the intellectual property rights

지도교수 이 상 원

이 논문을 이학석사 학위논문으로 제출함

2016년 12월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학

김 지 아

김지아의 석사학위논문을 인준함

2016년 12월

위 원 장 _____ (인)

부 위 원 장 _____ (인)

위 원 _____ (인)

요약(국문초록)

오늘날 소프트웨어의 무형적 자산 가치는 점차 증가하고 있다. 소프트웨어 산업이 정치, 경제, 사회 전반에 미치는 영향력 또한 점차 커져 감에 따라, 국제조약을 비롯한 입법과 행정의 전 분야에서 온라인상의 소프트웨어 불법 복제 방지 방안에 대해 깊이 있는 논의가 진행되고 있다. 그러나 정작 그 법규와 지침 등을 구체적으로 적용하는 준사법기관인 검찰은 이 분야에 대한 깊이 있는 이해 부족으로 초기 수사에서 형사처벌을 위한 증거수집 방법이 허용되는 경계도 확정짓지 못하는 경우가 많다. 실무상 다양한 사례의 소프트웨어 불법 복제, 무단 사용으로 인한 저작권 침해의 고소장이 접수되고 고소인은 증거 삭제의 용이성을 이유로 신속하고 기밀하게 압수수색영장을 발부받아 추가 증거를 수집하고 공소를 제기하여 형사처벌해 줄 것을 요청하지만, 고소인의 증거수집 절차에 위법성은 없었는가, 영장청구로 나아가도 될 것인가를 판단하는데 도움이 될만한 대검 차원의 구체적이고 통일적인 지침도 없다. ① 글로벌 시장을 가진 소프트웨어의 특성상 국내에서 사용되는 소프트웨어의 상당수가 외국기업이 저작권을 가지고 있는데 이들이 국내 로펌에 저작권침해 사범에 대한 고소를 위임한 경우, 구체적인 소프트웨어의 명칭 및 그로 인해 침해당한 저작권의 종류, 피혐의자 등이 특정되어 있지 않은 채로 작성되는 일괄적인 위임장에 근거한 고소장을 고소권자의 유효한 고소라고 보고 수사를 개시할 수 있는가의 문제, ② 저작권자인 사인이 일명 크랙정보 수집 프로그램을 사용해 불법 소프트웨어 사용자의 통신사실 확인자료를 수집하여 피의자를 특정한 경우, 이는 통신비밀보호법에 저촉되는 것으로 위법한 증거가 되는 것은 아닌가의 문제, ③ 압수수색영장을 발부받아 고가의 소프트웨어를 불법 복제하여 사용하는 중소형 기업 사무실의 컴퓨터 장비를 압수수색한 결과, 현장에서 고소의 대상이 아니었던 다른 개발사가 저작권을 가진 소프트웨어 역시 무단으로 불법복제하여 사용되고 있는 것을 알았을

때, 이를 친고죄인 저작권법 위반의 현행범으로 보고 영장없이 긴급 압수수색하고, 사후영장을 청구할 수 있는가의 문제 등 소프트웨어 관련 저작권침해 사범 수사와 관련해 실무상 다양한 문제가 쟁점이 되고 있고, 이를 위해 현행법률 조문 구조 및 그 의미에 대한 체계적인 이해와 합리적인 법개정, 적법한 수사관행 확립이 필요하다.

본 논문에서는 이중, 저작권자가 특히 크랙정보 수집 프로그램을 활용해 수집한 불법 사용자의 IP 주소, MAC 주소 등을 바탕으로 피의자를 특정하여 고소한 경우, 이를 적법한 증거로 하여 압수수색 영장 청구를 위한 혐의가 소명되었다고 볼 수 있을지 여부에 대해 주로 검토하며, 현행법률 해석상 허용되지 않는다면, 저작권의 재산적 권리를 보호하기 위하여 입법을 통해 근거규정을 구비할 필요성에 대해 검토하고, 다만 기술적 보호조치에 대한 보호가 그 본래 목적인 저작권 자체로 보호하고자 하는 권리 이상을 창설하여 소프트웨어 사용자의 프라이버시 등을 지나치게 침해하고 저작권의 공정 이용 및 과학기술 발전에 걸림돌이 되는 불합리한 경우를 막고자 그 소프트웨어가 가진 기술적 보호조치의 보호 정도에 따라, 저작권자의 사적인 증거수집을 허용하고 이를 수사기관에 제공할 수 있도록 법률적 보호를 차등화하는 방안을 제안하고자 한다.

주요어 : 소프트웨어 불법복제, 저작권 침해, 크랙정보, 통신비밀보호법, 통신사실 확인자료, 기술적 보호조치
학 번 : 2016-26061

<차례>

<표 목차>

Ⅰ. 서론

1. 소프트웨어 불법복제 문제 대두

21세기 정보화 사회의 정보기술의 발전은 눈부시다. 네트워크의 고속화, 기록매체의 대용량화에 따라 디지털 저작물 역시 급속도로 증가하며 인간의 업무와 생활에 점차 관련성을 미치고 있고 그 결과, 생산, 유통, 소비의 전과정에 걸쳐 저작권의 영향력이 지속적으로 확대되고 있다. 또한 오늘날 지식기반사회에서 유형적인 물질의 가치보다 무형적인 정보의 가치가 중요시되고, 비물질적인 생산요소가 주목을 받으며 소프트웨어 개발 기술은 비단 산업 뿐 아니라 정치, 경제, 문화의 전 영역에 걸쳐 국가 경쟁력 제고에 기여하는 중요한 분야로 각광받고 있다.

그에 따라 소프트웨어의 저작권을 보호하려는 국제적인 규제와 정부차원의 관리와 지원이 이루어지고 있음에도, 일반 기업 및 개인들 사이에서는 여전히 별다른 범죄의식 없이 소프트웨어를 불법적으로 사용하거나, 복제해서 사용하고 있다. 이는 소프트웨어 자산의 범위가 모호할 뿐만 아니라, 복사 및 설치가 쉽고 눈에 보이지 않아 관리자체가 어려운 소프트웨어 자체의 특성 때문[1]이기도 하지만 법과 제도를 비롯한 사회의 외연으로 확장하여 거시적인 관점에서, 혹은 한 개인의 내면에 주목하여 미시적인 관점에서 그 원인을 분석해 볼 수도 있다.

2. 기술적 보호조치와 그 무력화 기술의 발달

소프트웨어 불법복제를 막기 위해 오늘날 저작권자는 소프트웨어의 불법적인 이용 및 복제를 통제하기 위해 기술적 보호조치(technological protection measure: TPM)를 취하고 있다. 기술적 보호조치가 발전함에

1) 차태원, 안재경, “소프트웨어 자산관리를 위한 패키지소프트웨어 점검서비스 구현”, 「정보처리학회논문지」 제16-D권 제1호(2009. 2), 123면.

따라 이를 무력화하려는 시도 또한 발전하고 있는데, 컴퓨터 소프트웨어에 대한 불법 조작 및 변조 등의 행위를 일명 '크랙(Crack)'[2]이라고 한다. 소위 '소프트웨어 해커'라 불리는 크래커(Cracker)들은 인터넷이 활성화됨에 따라 자신들의 노하우를 국제적인 교류를 통해 손쉽게 공유할 수 있게 되었으며 단순한 도구나 역공학(reverse engineering)[3]을 이용한 크래킹을 통해 자신들의 요구에 맞도록 프로그램 코드를 수정하거나 무력화시킬 수 있게 되었다.[4]

아날로그 환경에서 저작권자들이 적용시킨 기술적 보호조치도 물리적, 유형적인 방법 등으로 무력화될 수 있었으나 무력화 행위 그 자체를 규율할 필요성이 상대적으로 적었다. 하지만 디지털 형태의 저작물에 적용된 기술적 보호조치가 무력화될 경우 그 피해규모 및 파급효과는 아날로그 환경과는 비교할 수 없을 정도로 크기 때문에[5] 기술적 보호조치를 무력화시키는 행위에 대한 규제의 필요성이 대두되었고, 이를 입법으로 규제하기에 이르렀다.

3. 형사고소를 통한 저작권 보호

입법적 규제에도 불구하고, 기술적 보호조치의 무력화 시도는 끊임없이 이루어지고 있다. 끝없이 진보하는 과학기술의 특성상 어떠한 기술적 보호조치도 스스로를 온전히 보호할 수 없기에, 무력화 시도로부터 자유로울 수는 없을 것이다. 이에 소프트웨어 저작권자들은 침해를 불가능하게 하는 기술적 보호조치 개발을 목표로 하기보다 저작권을 침해하는 사용자

---

2) 게임, 유틸리티 등의 소프트웨어에서 복사금지, 실행금지 등의 기술적 보호장치를 깨는 파일을 가르키기도 하고, 그러한 행위 자체를 일컫기도 함

3) 소프트웨어를 분석하고 동작을 해명해 나가는 것, 본래 대상이 되는 기계를 분석하고 동작을 관찰하여 제조방법, 동작원리, 설계도 등을 조사하는 행위를 말하나 소프트웨어에 대해서는 주로 역어셈블러한 코드의 해독 및 디버거로 소프트웨어 동작을 분석하는 일 등을 말한다(愛甲健二, "리버스 엔지니어링 입문, 즐거운 리버싱", 비제이퍼블릭(2014. 10.) 제9면.

4) 김요식, 윤영태, 박상서, "윈도우 환경에서의 메모리 해킹 방지 시스템 연구", 「정보보증논문지」 제5권 제3호 (2005. 9.) 제76면.

5) 김병일, "인터넷상의 저작물 불법유통에 대한 규제방안", 「法學論叢」 제33권 제2호(2009), 198면.

를 적발하고, 처벌할 수 있도록 증거를 수집하는 방향으로 기술적 보호조치를 발전시키고 있다. 그 한 예가 크랙정보 수집 프로그램을 활용하는 것이다. 특정 소프트웨어의 라이선스 파일은 레지스트리에 위치해 정품 사용자의 고객번호, 주소, 이름, 이메일 등과 사용승인 받은 모듈을 기재하고 있다가, 사용자가 프로그램을 실행할 때마다 이를 검토해서 정품사용자인지 여부를 자동으로 체크하고, 만일 이를 무력화하고 불법 복제된 프로그램을 사용하면 그 사용자의 IP 주소, MAC 주소, 도메인 등(일명 '크랙정보')을 수집하여 소프트웨어 개발사의 서버에 보내준다. 개발사에서는 이 정보를 바탕으로 해당 IP 주소를 할당받아 사용하는 기업체 내지는 개인의 주소지 등을 특정하여 해당 사용자가 정품을 구매한 내역이 없음을 확인하고, 수사기관에 형사고소를 한다. 이때 통상 고소인으로서는 프로그램 삭제 등을 통해 쉽게 증거인멸이 가능한 소프트웨어 불법복제의 특성을 이유로 증거확보를 위해 압수수색영장을 발부받아 불시에 사용현장을 단속하여 실행위자를 특정해 줄 것을 요구한다.

4. 사인이 수집한 크랙정보를 바탕으로 한 압수수색영장 청구의 문제

현행 저작권법이 지적재산권 침해 범죄에 대해 친고죄를 채택[6]하고 있어, 저작권자의 고소 없이는 수사를 개시할 수 없는 상황에서 수사의 속행여부는 개발사, 즉 저작권자의 고소 및 제출 증거에 의존할 수 밖에 없으므로 저작권자가 제시하는 '크랙정보'는 초기 수사 단계에서 강제수사인 압수수색영장 청구 여부를 결정하는 유일한 증거가 되곤 한다. 형사소송법 제215조 제1항은 '검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수

6) 저작권법 제 140조, 다만 제1호 단서에서 '영리를 목적으로 또는 상습적으로'의 경우 예외규정을 두고 있으나, 실무상 소프트웨어의 불법 복제 및 유포 그 자체를 업무로 하는 경우가 아니라면, 대부분의 기업체에서 특정 설립목적에 따라 업무에 필요한 범위중 하나로 수개의 소프트웨어를 사용하는 것 자체는 '영리를 목적으로'에 해당한다고 보지 않으며, 수사의 개시 전 단계에서 특정 IP 주소에서의 특정 소프트웨어 수회 사용 사실만으로 '행위자의 속성'인 '상습성'을 인정하기는 어려우므로 친고죄의 적용이 배제될 것을 전제하고 수사를 개시하는 경우는 거의 없다.

있는 것에 한정하여 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다'고 하여 압수수색영장 청구를 위해서는 최소한의 '죄를 범하였다고 의심할 만한 정황'에 대한 소명을 요구한다. 이는 불법 소프트웨어 사용 저작권법위반 혐의에 대한 압수 수색 과정이 피의자의 컴퓨터에 검색용 프로그램을 설치해서 불법복제 소프트웨어 사용여부를 검색하는 것으로 단시간 내에 그 절차가 끝나고, 피의자의 점유하에 있는 유형의 물건을 가져올 필요가 없어 일반적인 압수 수색에 비해 피의자의 기본권을 크게 침해하거나 사유재산에 피해를 야기할 우려가 크지 않다고 하여도 달리 볼 바 아니다.

5. 연구 방향 및 내용

따라서 본 논문에서는 위와 같이 불법 복제 소프트웨어 사용 의심자의 IP 주소, MAC 주소, 도메인 등을 수집하여 전달하는 일명 '크랙정보 수집 프로그램'을 사용해 취득한 IP 주소 등이 저작권법 위반 혐의의 유일한 소명자료일 때, 이를 토대로 수사기관은 압수수색영장 신청 내지는 청구로까지 나아갈 수 있는지에 대한 검토를 하고자 한다. 그 전 단계로, 소프트웨어의 기술적 보호조치의 예, 보호조치의 무력화를 시도하는 크래킹 기술에 대한 이해의 폭을 넓히고 크랙정보 수집 프로그램의 원리, 크랙정보 수집 프로그램 활용의 문제점, 통신사실 확인자료 제공을 금지하는 현행 통신비밀보호법의 해석 및 규율대상 등에 대해서도 검토한 후 그 문제점과 바람직한 향후 방향 등을 논의해 본다.

Ⅱ. 소프트웨어 불법복제와 기술적 보호조치

1. 소프트웨어 불법복제의 의의

소프트웨어 불법복제란, 저작권자의 허락 없이 컴퓨터 소프트웨어를 무

단으로 복제하여 사용하는 것을 말한다.

저작권법 제2조 제16호는 '「컴퓨터프로그램저작물」은 특정한 결과를 얻기 위하여 컴퓨터 등 정보처리능력을 가진 장치(이하 "컴퓨터"라 한다) 내에서 직접 또는 간접으로 사용되는 일련의 지시·명령으로 표현된 창작물을 말한다.'라고 하고, 제22호에서 '「복제」는 인쇄·사진촬영·복사·녹음·녹화 그 밖의 방법으로 일시적 또는 영구적으로 유형물에 고정하거나 다시 제작하는 것을 말하며, 건축물의 경우에는 그 건축을 위한 모형 또는 설계도서에 따라 이를 시공하는 것을 포함한다.'라고 정의하고 있다. 또한 저작권법 제136조 제1항 제1호는 벌칙규정에서 '저작재산권, 그 밖에 이 법에 따라 보호되는 재산적 권리를 복제, 공연, 공중송신, 전시, 배포, 대여, 2차적 저작물 작성의 방법으로 침해한 자'를 처벌한다고 하고 있다. 비록 위 처벌규정이 복제를 그 한 행위 태양으로 언급하고 있지만, 복제행위 그 자체만으로는 처벌받는 위법행위라고 단정할 수 있는 것은 아니다.

왜냐하면 통상 구매 또는 라이선스 구입 등으로 사용권을 취득한 소프트웨어는 개인적인 목적으로 복제하는 한 구매자의 사용권의 범위[7] 안에 있는 행위로 허용되기 때문이다. 다만, 복제한 것을 허가되지 않은 이에게 배포한다면 그 배포하는 행위가 불법에 해당된다. 또한 이를 복사해서 사용하는 사용자는 불법 소프트웨어 사용자가 된다. 따라서 불법인지 여부는 복제라는 행위 자체가 아니라 허용된 사용범위를 초과해 저작권자의 저작재산권 등을 침해하였는지 여부에 따라 결정된다.

2. 소프트웨어 불법복제의 원인

7) 오늘날은 구매자의 사용권의 범위 역시 제한하여 특정 소프트웨어의 경우 복제할 수 있는 한도를 2-3개의 컴퓨터로 한정하는 예도 많다. 아이폰, 안드로이드폰, 아이패드, 윈도우 컴퓨터, 애플 컴퓨터 등 다양한 기기간에 동기화를 해서 사용할 수 있는 글쓰기 어플인 '에버노트'의 경우 무료 사용자는 모든 기기를 통틀어 2개의 기기에서만 어플을 사용할 수 있게 제한하는 방식이다.

소프트웨어 불법복제의 원인을 설명하는 두 가지 관점이 있다. 국가간의 불법복제율 차이에 주목하여 한 사회의 경제력 정도나 법적, 제도적 장치의 유무, 문화적 요인 등을 통해 불법복제율을 설명하려는 거시적인 관점과 불법복제가 개인의 행동이란 점에 착안해, 불법복제의 환경적 유인과 도덕성 등 개인적 차원에서 불법복제를 설명하려는 미시적인 접근 시도가 그것이다.[8)]

가. 소프트웨어 불법복제를 설명하는 거시적 요인

불법복제에 영향을 미치는 변수는 크게 경제적 요인, 사회·문화적 요인, 법적·제도적 요인, 기술적 요인으로 구분할 수 있다.

1) 경제적 요인에 주목하는 관점

저작권은 재산권의 인정이라는 자유경제의 원칙 아래에서 보호받을 수 있으므로 자유경제 체제의 발달과 개방 경제로의 편입은 저작권이나 특허권의 보호를 더욱 강조함으로써 간접적으로 불법복제율을 낮추는 역할을 한다고 주장한다. 실제로 통계상으로도 국가의 소득수준이 높을수록 낮은 불법복제율을 보이고 있다.

국내 총생산뿐만 아니라 국가 안에서 소득분배 구조도 불법복제에 영향을 미치는 요인이 될 수 있다. 국민총생산이 높아 소득수준이 높은 국가라 할지라도 소득분포가 불균형을 이룬다면 정품 콘텐츠를 구입할 수 있는 국민은 많지 않아 콘텐츠를 불법복제 할 유인이 존재한다.

2) 사회·문화적 요인을 강조하는 관점

개인의 지적 창작물에 대한 동·서양의 태도 차이에 주목하여 서양 사회에서는 지적 창작물의 소유권을 개인이 갖는 것으로 생각하는 반면 동양에서는 창작물이 사회의 발전과 복지를 증진시키기 위해 이용되어야 한다

8) 유진룡, 「엔터테인먼트 산업의 이해」, 넥서스 비즈, (2009), 499면 이하; 김상겸, “게임소프트웨어 불법복제에 관한 법적연구” (2014) 17면.

는 생각이 지배적이기 때문에 동양이 불법복제에 대해 서양보다 관대해 불법복제율이 더 높다고 주장하는 시각도 있다.[9)]

3) 법적・제도적 요인으로 설명하는 관점

저작권법의 존재여부, 베른 협약과 파리협약 등 IR 보호 협약, 국제저작권협회의 회원 가입 여부 등 불법복제와 같은 지적재산권을 보호하는 법적, 지적재산권 보호의 존재 여부와 IT 산업에 대한 무역규제, 관료제도의 효율성, 정부 효율성 지표 등 제정된 법이나 규제 등의 효과적인 집행 가능성 여부, 지적재산권 보호제도의 유무에 따라 불법복제율이 달라진다고 주장하는 시각도 있다.

4) 기술적 요인에 주목하는 관점

경제적 요인이나 문화적 요인, 법적, 규제적 요인이 불법복제에 대한 사회 전반적인 분위기 형성에 간접적으로 이바지하여 불법복제 의도에 영향을 미치는 것에 비해 기술적 요인은 실제 불법복제를 하거나 정품을 사용할 때 행동의 용이성에 직접 영향을 미침으로써 불법복제를 결정하는 요인이 된다고 보는 학자도 있다. 불법복제의 형태가 컴퓨터 구입처나 지인을 통해 이뤄지는 때도 있지만 상당부분 인터넷의 웹하드 사이트와 토렌트 등 P2P[10)]서비스를 통해 이뤄지고 있음[11)]을 고려할 때, 불법복제율은 인터넷 이용률이나 광대역 인터넷망 확산에 따라 증가할 것으로 예상할 수 있다.

나. 소프트웨어 불법복제를 설명하는 미시적 요인[12)]

---

9) Depken and Simmons 2004; Shin, Gopal et al. 2004; Bagchi, Kirs et al., 2006.

10) peer to peer, 인터넷에서 개인과 개인이 직접 연결되어 파일을 공유하는 것을 이야기한다. [네이버 지식백과] P2P (두산백과) 참조

11) 전자신문 2014. 10. 17.자 기사, 소성렬 기자 “저작권문화발전연구소, “위디스크 등 웹하드, 음란물과 불법 콘텐츠의 천국”, http://www.etnews.com/20141017000308 (2016. 11. 10. 최종확인)

12) 김광용, “소프트웨어 불법복제에 따른 경제적 효과분석 및 정책방향 제시”, 「프로그램심의조정위원회 연구보고서」(2002. 4.)

나이와 성별 등 일정한 인구통계적 특성에 따라 불법복제라는 행위를 할 가능성이 달라진다는 가설 하에 나이가 어릴수록, 사회적 지위가 낮을수록, 교육수준이 낮을수록 불법복제를 할 가능성이 커진다는 연구결과[13]가 있다.

또한 경제학의 사회적 교환이론에 따라, 불법복제는 정품이용자와 불법복제자간 거래가 전제된다는 점에 주목하여 거래가 일어나는 주체들에게 상호간 이익이 발생할 때 불법복제가 일어난다고 보는 견해도 있다. 사회적 교환이론은 대부분 공정성 이론을 통해 설명하는데, 불법복제에 참여하는 두 교환자가 서로의 투입에 비해 성과가 더 크다고 인식할 때 거래가 성립한다는 것이다. 즉 콘텐츠의 가격이 오를 때 교환에서 투입의 가치가 높아지기 때문에 산출가치가 함께 높아지지 않는 한 다른 사람에게 빌려줄 의도가 낮아진다고 한다. 빌려주려는 콘텐츠의 가격이 높을수록 그만큼의 가치를 돌려받을 가능성이 작아 불법복제 콘텐츠를 제공하려는 유인이 낮아진다는 것이다.[14] 그러나 실제로 요즘처럼 불법복제 콘텐츠가 인터넷을 통해 유통되는 환경에서 프로그램 제공자는 수혜자로부터 경제적 보상을 받으려 한다고 보기 어렵고, 불법복제가 일어나는 대부분의 경우 제공되는 콘텐츠는 그 역시 정품이 아닌 불법복제품일 가능성이 크기 때문에 가격이 높다고 해서 불법복제가 일어나지 않을 것이라는 예측은 타당성이 약하다는 지적도 있다.

그 밖에도 불법복제라는 행동은 그와 관련된 다양한 상황적 변수-콘텐츠의 구입용이성, 가격, 홍보 및 교육, 처벌의 위험 등과 같은 상황적 요인-에 의해 영향을 받을 수 있다.

3. 소프트웨어 불법복제의 실태

1994년 불법복제율 75% 정도로 매우 심각한 상황이었던 우리나라의 불

---

13) Susan J. Harrington., "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions", Mis Quarterly, Setember, 1996, pp.257-278

14) Glass, R. S. & Wood, W. A., “Situational Determinants of Software Piracy: An Equity Theory Perspective.” Journal of Business Ethics, 15, 1996, pp. 1192-1193.

법복제 실태는 소프트웨어 산업의 육성이라는 기치 하에 1999년도부터 집중단속에 들어간 이후 불법복제율이 꾸준히 줄어들어 2002년도에 50%까지 감소하였다.[15]

연도	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
침해건수 (건)	1,311	1,893	2,033	2,387	1,448	1,055	1,096	967	765	755	614
침해액 (백만원)	30,586	36,337	48,101	55,972	34,729	35,637	35,163	49,532	59,238	43,127	47,926

[표 1] 연도별 소프트웨어 저작권 침해 상황[16]

위 표에서 보듯 우리나라는 2000년대 초반 이후로 소프트웨어 관련 저작권 침해가 점차 증가하는 추세에 있었으나, 지속적인 계몽과 정부 차원의 규제 등에 힘입어 2010년[17]을 전후하여서는 침해건수 자체는 크게 줄어드는 모습을 확인할 수 있다. 다만 침해건수가 줄어들었음에도 불구하고 그 피해 액수는 오히려 더 커지고 있어 개별 침해사건의 규모가 커지고 있는 것으로 보인다.

결국 일반 국민들의 저작권에 대한 인식이 제고되었고, 지적재산권의 가치를 중요시 하는 사회분위기가 확산되었음에도 여전히 소프트웨어 저작권 침해는 활발히 이루어지고 있음을 알 수 있다.

4. 기술적 보호조치

가. 기술적 보호조치의 개념

15) 정완 “소프트웨어 불법복제 실태와 법제도적 개선방안”, 한국형사정책연구원 (2003. 12.), 제11면.
16) 한국소프트웨어 저작권협회 홈페이지 http://www.spc.or.kr (2016. 9. 27. 확인)
17) 2010년은 국제거래에서 위조 및 불법복제 문제에 보다 효과적으로 대응하기 위해 지적재산권 집행의 통일된 기준 등을 마련한 국제규범인 위조및불법복제방지협정(Anti-Counterfeiting Trade Agreement, ACTA)가 최종타결된 해이기도 하다.

기술적 보호조치란 저작권자가 자신의 저작권을 사전에 방어적으로 보호하기 위하여 스스로 강구하는 기술적 자구조치라고 할 수 있다. 디지털 환경 하에서는 일단 한번 저작권이 침해되어 복제물이 인터넷상에 공개되고 나면 그 피해가 걷잡을 수 없이 확산되어 사후적인 구제수단으로는 피해를 보전하는 것이 사실상 불가능하게 됨에 따라 기술적 보호조치의 중요성은 나날이 더해가고 있다.

나. 기술적 보호조치의 분류[18)]

1) 통제대상에 따른 분류

기술적 보호조치는 이를 통해 통제 내지 보호하려는 대상, 즉 저작물의 이용양태에 따라 접근통제조치(access control)와 이용통제조치(copy control)로 나누는 것이 일반적이다.

(1) 접근통제조치

접근통제조치는 저작권의 침해와 관계없이 저작물에의 접근 자체를 통제하기 위한 기술을 말하며, '이용'하기 위하여는 '접근'이 먼저 전제되어야 한다는 점에서 근본적으로 정보에 대한 통제중 가장 강력한 것이다. 여기서의 '접근'은 두 가지로 나뉘어 설명되고 있는데, 첫째 서버 또는 그와 같은 저작물의 원본이나 복제물을 담고 있는 매체에 접근하는 것이고, 둘째 저작물의 복제물을 재생하여 그에 포함된 저작물의 내용에 접근하는 것으로 이는 실질적으로 저작물을 사용(use), 향유(enjoy), 또는 체험(experience)하는 것을 의미한다.

디지털 시대 이전에는 '접근'에 대한 통제 없이도 저작권자는 오프라인에서 유체물에 대한 물리적인 소유권에 기초하여 사실상 불법사용을 통제할 수 있었는데, 수록매체에의 접근통제만으로도 대부분의 경우 저작물에의 통제를 이룰 수 있었기 때문이다. 그러나 디지털시대가 도래하면서 접근

18) 이규홍, "저작권법상 기술적 보호조치의 법적 보호에 관한 연구", 「연세 의료·과학기술과 법」 제1권 제1호 (2010. 2.) 59면.

을 통제할 수 있는 사실상의 능력은 축소되었고 무단접근으로 인한 피해는 광범위하게 이루어지게 되었다. 이에 따라 오프라인 세계에서 저작권자가 가지고 있었던 사실상의 통제력이 디지털 환경에서 회복되어야 한다는 즉, 접근의 개념을 확대하자는 주장이 나왔다.

그러나 접근통제조치는 이미 저작권자의 배타적인 권리에서 벗어나 공유부분에 있거나 저작권이 소멸된 저작물을 보호하기 위하여 설치된 경우도 아예 접근자체가 방지되는 결과를 초래하므로 저작권법이 저작권자의 권리보호와 함께 추구하는 '공정 이용'의 이념에 반할 우려가 있고, 표현의 자유 등 다른 헌법적 가치를 심하게 침해할 우려가 제기되며, 기술발전을 억제하는 부작용이 있을 수 있다는 점에서 논란의 대상이 되었다.

(2) 이용통제조치

이용통제조치는 저작물에의 접근 자체를 제한하는 것은 아니지만 복제 등 이용을 통제함으로써 저작권의 침해행위를 방지하는 기술로서, 이미 '접근'한 것을 전제로 한 것이다. 여기서의 '이용'은 저작권자의 허락을 필요로 하는 저작물의 이용행위를 말하며, 구체적으로는 저작권을 구성하는 각각의 지분권의 대상이 되는 행위, 즉 복제, 공연, 방송, 배포, 전송행위 등이 이에 해당한다.

2) 금지범위에 따른 분류

금지되는 행위의 범위에 따라 ①기술적 보호조치를 직접 무력화하는 행위를 금지하는 입법(이하 '직접적 무력화행위 금지'), ②기술적 보호조치를 무력화하기 위하여 사용되는 도구(기술, 서비스, 제품, 장치 또는 그 주요부품 등)의 제공 등 거래행위를 금지하는 입법(이하 '간접적 무력화행위 금지')으로 구분된다. 어느 유형의 무력화 행위를 금지시킬 것인지는 중요한 입법정책의 표출일 것인데 이론적으로 확립된 원칙은 없다.

다. 기술적 보호조치에 대한 조약 및 주요국가의 입법례[19)]

1) 기술적 보호조치의 입법

1996년 세계지적재산권기구(World Intellectual Property Organization, 이하 'WIPO') 저작권조약(WIPO Copyright Treaty, 이하 'WCT')과 WIPO 실연음반조약(WPPT)에서 최초로 기술적 보호조치의 무력화를 규제하는 입법을 시작했다. WCT 제11조는 "체약 당사국은 본 조약 또는 베른협약에 따라 저작자가 권리를 행사하는 것과 관련하여 사용하는 효과적인 기술적 보호조치와, 저작물에 관하여 저작자가 허락하지 아니하거나 법에서 허용하지 아니하는 행위를 제한하는 효과적인 기술적 보호조치를 무력화시키는 것에 대하여 적절한 법적 보호와 효과적인 법적구제수단을 제공하여야 한다"고 규정하여 저작물 일반에 대한 기술적 조치의 무력화를 금지할 것을 조약의 내용으로 하고 있다. 그러나 WCT는 접근통제에 관해서는 명시적으로 규정하고 있지 않다. 다만, 보호의 대상, 규제대상 및 구제방법 등에 관한 구체적인 규정은 각국의 재량에 맡기고 있다.

2) 주요 외국의 입법동향[20]

(1) 미국의 DMCA(Digital Millenium Copyright Act)

미국의 밀레니엄디지털저작권법은 연방저작권법에 수용되어 있는데, 연방저작권법 제1201조는 '저작권보호시스템의 우회'라는 표제하에 구체적인 규정을 두고 있다. 이 규정에 의해 법적 보호의 대상이 되는 기술적 보호조치는 저작물에 대한 접근을 통제하기 위한 기술조치와 저작권을 보호하기 위한 기술조치이다. 즉 제1201(a)(1)은 저작권자에 의해 그들의 저작물에 대한 접근을 효과적으로 제어하기 위하여 사용되는 기술적 보호조치들을 우회하는 것을 금지하며, 제1201(a)(2),(b)는 기술적 보호조치들을 우회할 목적으로 설계되거나 생산된 기술 및 장치들의 제조 및 배포를 금지하고 있다. 이와 같이 저작물에의 접근통제의 회피가 금지됨으로써 저작물

19) 김병일, "인터넷상의 저작물 불법유통에 대한 규제방안", 「法學論叢」 제33권 제2호(2009), 198면.

20) 탁희성, "저작권 보호를 위한 기술적 보호조치에 관한 소고", 「형사정책연구」 제20권제1호(2009), 1233면.

에 대한 접근을 통제하는 권리 즉 '접근권'이 결국 저작권자에게 인정되는 결과를 가져오게 되었다.

이와 같은 저작물에의 접근은 본래 기존의 저작권법에 의해 보호되는 범위가 아님에도 불구하고 기술적 보호조치의 법적 보호를 통해 새로운 권리를 창설하고 있는 것으로 이용자가 저작물을 이용하기 이전 단계인 접근 자체를 통제할 수 있도록 법으로 인정한다는 것은 저작권자의 권리를 과대하게 강화시키는 것으로 저작권의 보호와 저작권의 제한이라고 하는 균형원리를 깨뜨린다는 비판을 받고 있다.

(2) 일본의 저작권법

2000년 1월부터 시행된 개정 저작권법 제102조의 2에서 I) 기술적 보호수단을 회피하는 것을 유일한 기능으로 하는 장치(당해 장치의 부품 1조로서 용이하게 조립될 수 있는 것을 포함한다) 또는 기술적 보호수단의 회피를 유일한 기능으로 하는 프로그램의 복제물을 공중에 양도하거나 대여 혹은 그러한 목적으로 제조·수입·소지하거나, 공중의 사용에 제공 또는 당해 프로그램을 공중에 송신하거나 송신 가능하게 한 자, ii) 업으로서 공중의 요구에 응하여 기술적 보호수단의 회피를 행한 자는 1년 이하의 징역 또는 100만 엔 이하의 벌금에 처한다고 규정하여 기술적 보호수단을 회피하는 전용장치 등을 공중에게 양도하는 등의 행위를 처벌하고 있다. 즉 무력화 행위 자체는 금지하지 않지만 그러한 행위를 가능하게 하는 무력화 예비행위에 대한 처벌규정을 두어 간접적으로 기술적 보호조치를 보호하는 방법을 취하고 있다.

(3) EU 정보사회 지침상의 기술적 보호조치 관련 규정[21]

「정보사회에서의 저작권 및 관련 권리의 조정에 관한 EC 지침(Directive 2001/29/EC of the European Parliament and of the Council of 22 May

21) 강기봉 "DRM기술을 둘러싼 개인정보 및 프라이버시의 법정책적 검토", 「법과 정책연구」 16권 2호, 한국법정책학회, (2016), 387면.

2001 on the harmonisation of certain aspects of copyright and related rights in the information society)」(이하 “EU 정보사회 지침”이라 한다)은 제3장 제6조에 기술적 보호조치에 관하여 규정하고 있다. 이 규정은 동조 제1호에 모든 기술적 보호조치에 대해 적절한 법적 보호를 할 것을 기술하고, 제2조에 특정한 조건 하에 기술적 보호조치의 무력화 예비행위에 대한 적절한 법적 보호를 할 것을 기술하였으며, 제3호에 기술적 보호조치의 정의를 하고 있고, 제4호에 기술적 보호조치의 무력화 금지에 대한 예외에 관하여 기술하고 있다. 그렇지만 이 지침은 기술적 보호조치의 보호와 관련한 법적 방향 내지 틀을 제시하는데 그치고, 구체적인 입법에 대하여는 각 국가에 맡기고 있다.

3) 우리나라의 입법경향

국제적 차원에서는 WCT가 처음으로 기술적 보호조치의 보호의무를 규정하였는데, WCT의 기술적 보호조치 보호 의무에 앞에서 말한 접근통제적 기술조치가 포함되는지 여부에 대해 견해의 대립이 있지만, 2010. 12 타결된 한미 FTA(2012. 3. 15. 발효)에서 명시적으로 접근통제적 기술조치를 보호하기로 합의하였기 때문에 저작권법에 접근통제적 기술조치를 반영하는 개정(일부개정 2011. 6. 30. 법률 제10807호, 일부개정 2011. 12. 2. 법률 제11110호)이 이루어졌다. 종전 저작권법 제2조 제28호 기술적 보호조치 정의 규정[22]에 기존 이용통제 외에 접근통제를 추가하고, 제104조의2에서 접근통제 기술적 보호조치를 포함한 기술적 보호조치의 무력화 금지 규정을 신설한 것이다.

저작권법 제2조 제28호 가목은 접근통제 기술적 보호조치, 나목은 이용통제 기술적 보호조치를 의미한다. 이러한 기술적 보호조치의 예는 사용

22) 저작권법 제2조 제28호 기술적 보호조치
가. 저작권, 그 밖에 이 법에 따라 보호되는 권리의 행사와 관련하여 이 법에 따라 보호되는 저작물 등에 대한 접근을 효과적으로 방지하거나 억제하기 위하여 그 권리자나 권리자의 동의를 받은 자가 적용하는 기술적 조치.
나. 저작권, 그 밖에 이 법에 따라 보호되는 권리에 대한 침해 행위를 효과적으로 방지하거나 억제하기 위하여 그 권리자나 권리자의 동의를 받은 자가 적용하는 기술적 조치.

권한 제어기술(Use Control), 복제방지기술(Copy Protection), CAS 등의 기술, 암호화 기술(Cryptography), 키 관리(Key Management) 등[23]이라 할 수 있다. 개정 전의 구 저작권법은 제124조 제2항에 기술적 보호조치에 대한 무력화행위의 금지 및 처벌 등을 규정하며 기술적 보호조치 무력화행위 자체는 금지하지 않고, 그와 같은 무력화를 주목적으로 하는 기술·서비스·제품·장치 또는 그 주요 부품을 제공·제조·수입 하는 것과 같은 무력화 예비행위를 금지하고 있었고, 단서나 예외조항으로 저작권 제한 또는 공정 이용에 관한 규정을 준용하지 않았기 때문에 기술적 보호조치 침해행위에 대해서는 공정 이용의 예외가 적용되지 않는다고 해석할 수 밖에 없었다. 그러나 접근통제 기술적 보호조치에 대한 지나친 보호는 공정하게 저작물을 이용하려는 사람들이 저작물에 접근하는 것까지 제한하게 되어 저작물의 공정한 이용을 저해할 우려가 있고, 저작권을 보호함과 동시에 제한함으로써 저작권자의 사적인 권리와 사회문화의 발전이라는 공익을 함께 추구하고자 하는 저작권법의 기본취지에 맞지 않으므로 저작권제한에 관한 규정이 기술적 보호조치의 보호에 관한 규정에 있어서도 일관되게 적용될 수 있도록 명문화할 필요가 있다는 지적에 따라 현행 저작권법은 위 법률 단서조항으로 기술적 보호조치의 무력화가 정당화되는 경우[24]를 열거하고 있다.

---

23) 강기봉 “DRM기술을 둘러싼 개인정보 및 프라이버시의 법정책적 검토”, 「법과 정책연구」 16권 2호, 한국법정책학회, (2016), 380면.

24) 1. 암호 분야의 연구에 종사하는 자가 저작물 등의 복제물을 정당하게 취득하여 저작물 등에 적용된 암호 기술의 결함이나 취약점을 연구하기 위하여 필요한 범위에서 행하는 경우. 다만, 권리자로부터 연구에 필요한 이용을 허락받기 위하여 상당한 노력을 하였으나 허락을 받지 못한 경우에 한한다.

2. 미성년자에게 유해한 온라인상의 저작물 등에 미성년자가 접근하는 것을 방지하기 위하여 기술·제품·서비스 또는 장치에 기술적 보호조치를 무력화하는 구성요소나 부품을 포함하는 경우. 다만, 제2항에 따라 금지되지 아니하는 경우에 한한다.

3. 개인의 온라인상의 행위를 파악할 수 있는 개인 식별 정보를 비공개적으로 수집·유포하는 기능을 확인하고, 이를 무력화하기 위하여 필요한 경우. 다만, 다른 사람들이 저작물 등에 접근하는 것에 영향을 미치는 경우는 제외한다.

4. 국가의 법집행, 합법적인 정보수집 또는 안전보장 등을 위하여 필요한 경우

5. 제25조제2항에 따른 교육기관·교육지원기관, 제31조제1항에 따른 도서관(비영리인 경우로 한정한다) 또는 「공공기록물 관리에 관한 법률」에 따른 기록물관리기관이 저작물 등의 구입 여부를 결정하기 위하여 필요한 경우. 다만, 기술적 보호조치를 무력화하지 아니하고는 접근할 수 없는 경우에 한한다.

라. 기술적 보호조치의 예[25]

1) DRM의 의의와 원리

DRM은 'Digital Rights Management'의 약자로, 소프트웨어 등 디지털 제품의 저작권 보호를 위해 콘텐츠의 사용을 제어하고, 불법복제 및 유통을 방지하는 기술 및 서비스를 의미한다. '디지털 저작권 관리' 혹은 '디지털 권한 관리'로 표현되기도 한다. 즉, 디지털 콘텐츠의 생성과 이용까지 유통 전과정에 거쳐 지적재산권을 보호하면서 콘텐츠를 안전하고 편리하게 배포할 수 있게 하는 기술과 서비스를 일컫는다.

DRM은 크게 협의의 DRM과 광의의 DRM으로 구분할 수 있다. 광의의 DRM은 디지털 콘텐츠의 생산, 분배, 거래규칙, 이용규칙, 과금, 거래내역의 관리 및 보고, 정산 등 디지털 콘텐츠의 전체 라이프사이클에 걸쳐 디지털콘텐츠의 지적재산권 보호와 디지털 콘텐츠 관리 및 유통 효율화를 위한 사용되는 기술과 서비스를 통칭하는 의미로 사용된다. 협의의 DRM은 불법복제 및 지적재산권 침해 행위로부터 디지털 콘텐츠를 보호해주기 위해 사용되는 기술이다.[26]

DRM은 디지털 콘텐츠에 사용하기 위해서는 반드시 저작권자가 배포하는 '라이선스'를 발급받아야 한다는 개념을 기술적으로 보장해주는 시스템이다. 세부적으로는 저작권 보호 대상인 디지털 콘텐츠는 배포 시에 이미 기술적인 보호 조치가 되어있는 상태이고, 사용자가 이 보호된 콘텐츠를 사용하고자 할 경우, 사용을 허가하는 라이선스를 획득한 이후에만 사용이 가능하도록 기술적 통제가 되어있는 시스템을 말한다. 이러한 DRM 기술은 아래에서 보는 바와 같이 여러 가지 방식이 있다.

---

6. 정당한 권한을 가지고 프로그램을 사용하는 자가 다른 프로그램과의 호환을 위하여 필요한 범위에서 프로그램코드 역분석을 하는 경우
7. 정당한 권한을 가진 자가 오로지 컴퓨터 또는 정보통신망의 보안성을 검사·조사 또는 보정하기 위하여 필요한 경우
8. 기술적 보호조치의 무력화 금지에 의하여 특정 종류의 저작물 등을 정당하게 이용하는 것이 불합리하게 영향을 받거나 받을 가능성이 있다고 인정되어 대통령령으로 정하는 절차에 따라 문화체육관광부장관이 정하여 고시하는 경우. 이 경우 그 예외의 효력은 3년으로 한다.

25) "SW 역분석과 기술적 보호조치(법적·기술적 재해석)", 「한국저작권위원회」(2009) 제47면.

26) 강호갑, "표준기술동향: DRM(Digital Rights Management)", TTA Journal, 제103호, 2006, 146면.

2) 디지털 저작물 위·변조 방지

디지털 저작물의 불법적인 위조나 변조를 검사하여 무결성을 증명하는 기술이다. 디지털 저작물 위·변조 방지를 위하여 다양한 기술 방식이 존재한다. 이러한 위·변조 방지 기술 방식에는 Built-in 방식, Plug-in 삽입 방식·OLE 제어 방식·File System Filter 제어 방식·VBA[27] 제어 방식 등이 존재한다.

소프트웨어의 이용권한을 통제하는 장치인 DRM Controller를 소프트웨어 내부에 응용 프로그램의 소스변경을 통해 특정 코드로 삽입해 주는 Built-in 방식과 일부 소프트웨어가 주된 기능에 영향을 끼치지 않는 범위에서 엔드유저가 자신의 필요에 맞게 인터페이스의 구성이나 색상, 배경이미지 등을 커스터마이징할 수 있도록 제공하는 plug-in ADK를 이용하여 DRM Controller를 개발하고, 이를 소프트웨어에 plug-in 형태로 제공하는 방식, OLE[28]를 통해 MS Office, AutoCAD, 훈민정음, 아래한글 2002 등과 같이 Active Document Server를 지원하는 프로그램 사이에서는 서로 다른 데이터의 양식을 다루면서도 데이터의 핵심구조를 공유하여 프로그램간 정보의 전송 및 공유가 가능하므로 DRM Controller는 OLE를 통해 Active Document sever의 각종 기능들을 통제하는 방식 등이다.

3) 디지털 저작물 패키징

디지털 저작물 및 저작권을 보호할 수 있는 형태로 구성하는 기술도 있다. DRM용 저작물 제작기술로 정의한다. Pre-Packaging은 사용자의 요청이 있기 전 EDMS[29], KMS[30], Groupware 등에 문서가 저장되기 전에

---

27) Visual Basic for application의 약어. 마이크로소프트 사의 윈도우 오피스 응용 프로그램용 매크로 언어. 동사의 제품인 비주얼 베이식을 기반으로 하여 매크로 언어를 범용화, 공통화한 것.[네이버 지식백과] VBA [Visual Basic for application] (컴퓨터인터넷 IT용어대사전) 참조

28) 윈도우에서, 데이터와 데이터를 연결하는 방법을 말한다. 연결된 데이터는 수정될 때 함께 수정되어 저장된다. 예를 들어, OLE가 지원되는 그래픽 프로그램에서 그림을 그린 후 문서 편집기와 연결시키면 나중에 그림이 바뀔 경우 문서 편집기의 그림도 같이 바뀐다. 이렇듯 OLE는 데이터 간의 정보를 연결시켜 준다. [네이버 지식백과] OLE [object linking and embedding] (두산백과) 참조

29) electronic document management system, 전자문서관리시스템, 다양한 형태의 문서와 자료를 그 작성부터 폐기에 이르기까지의 모든 과정을일관성 있게 전자적으로 통합 관리하기 위한

미리 저작물을 Secure Container로 패키징하는 방식이다. 이 방식으로 패키징된 지식정보들은 암호화되어 있기 때문에 기존 index 서버와의 연동이 어렵다는 제약점을 안고 있다.

4) 라이선스 처리

라이선스는 저작물의 이용에 대한 권한을 담고 있는 정보 단위로, 저작물에 대한 사용권한을 부여하기 위해 사용된다.

저작물의 이용을 위해서는 사용규칙 및 조건을 포함하고 있는 라이선스가 필요하다. 라이선스가 사용자의 PC에 존재하고 있으면 사용자는 저작물을 바로 이용할 수 있다. 만일 사용자의 PC에 라이선스가 없다면 저작물 제공업자의 시스템으로 라이선스 발급을 요청하게 된다. 라이선스 발급 요청시 사용자가 이용할 저작물의 식별번호와 사용자 정보 등이 저작물 제공업자의 시스템으로 전달된다. 저작물 제공업자의 시스템은 사용자로부터 전송된 정보를 이용하여 라이선스 발급 여부를 결정하게 된다. 만일 라이선스 발급요청을 한 사용자가 이미 해당 저작물에 대한 권한을 획득한 것으로 확인되면 새로운 라이선스를 발급하도록 한다.

유료 저작물인 경우, 저작물 제공업자는 저작물의 가격 및 이용 조건 등 저작물의 정보를 사용자에게 제시하고 이를 수락하는 사용자에게 라이선스 발급을 허락한다. 저작물 제공업자는 허가된 사용자에 한하여 적절한 사용권리 정보를 담고 있는 라이선스를 발급하게 된다. 라이선스에 포함되는 사용권리 정보는 사용권한(permission)과 사용조건(condition), 그리고 암호화된 저작물을 풀어볼 수 있는 암호화 키 정보 등이 포함되어 있다. 사용권한은 view/play, print, edit, extract, embed 등과 같은 저작물의 사용권한을 제어하는 정보를 담고 있으며, 사용조건은 저작물의 이용 회수 및 이용기간 등의 정보가 담겨지게 된다.

시스템 [네이버 지식백과] EDMS (두산백과) 참조

30) Knowledge Management System, 지식관리시스템, 기업내 조직구성원들이 축적하고 있는 개별적인 지식을 체계화하여 공유함으로써 기업경쟁력을 향상시키기 위한 기업정보시스템 [네이버 지식백과]KMS (매일경제) 참조

5) 키생성관리

디지털 저작물 보호를 위해 사용되는 암호기술의 안전성을 보장하기 위해서는 안전한 키관리 및 분배 매커니즘이 필요하다. DRM에서의 키 관리가 다른 암호시스템의 키 관리와 구별되는 가장 큰 특징은 저작물 전달 과정에 참여하는 유통업자, 분배자, 이용자 등 모든 사용자가 자신의 키를 알 수 없도록 관리되어야 한다는 점이다. 만약 자신의 키에 접근할 수 있다면 알고리즘의 비밀성이 보장되지 않는 한 저작물 원본을 뽑아내서 복제할 수 있기 때문이다. DRM 키 분배 방법은 대칭키 방식과 공개키 방식으로 구별될 수 있다.

대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 저작물 거래에 키 분배 서버가 관여해야 한다. 반면 공개키 방식을 사용할 경우 분산성, 확장성, 상호운용성 등에서 많은 장점을 갖게 되나, 공개키 기반구조(PKI)[31]가 필요하다는 부담이 있다.

그러므로, 저작물의 특성 및 적용 환경에 따라 적절한 키 관리 매커니즘을 선택하는 것이 바람직하다. 예를 들어 전자책, 음악 등과 같이 저작물 유통 범위가 광범위하고 저작물 유통 흐름에 많은 역할 개체들이 참여하는 경우, 하나의 키 분배 서버로 부하가 집중되는 키 관리 매커니즘은 적절하지 못하다 할 것이다.

6) 사용자 인증

저작물에 대한 사용 권리를 사용자별로 지정하고 통제하기 위해서 사용자 인증을 할 필요가 있다. 일반적으로 사용자의 인증처리를 위해 사용되는 기술은 ID/Password, Digital Certificate, SSO(Single-Sign-On), 생체인식 등이 있다. 이외에도 특정한 컴퓨터 또는 디바이스에서만 사용권한을 제어하기 위해 디바이스 인증 기술이 사용된다. 디바이스 인증 기술은

31) Public Key Infrastructure: 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템 환경을 말한다. 즉, 암호화와 복호화키로 구성된 공개키를 이용해 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템이다.[네이버 지식백과] 공개키기반구조 [PKI] (시사상식사전, 박문각)

CPU 일련번호나 통신카드의 MAC 주소, 그리고 HDD 일련번호 등과 같이 컴퓨터 또는 단말기의 고유한 식별정보를 바탕으로 사용자 정보와 결합하여 사용된다.

DRM은 특정한 인증기술에 종속될 필요는 없지만 적용 도메인 및 애플리케이션에 따라 적절한 인증기술과의 연동이 중요한 고려 사항이 된다. 따라서 DRM이 적용되는 응용 애플리케이션이나 적용 도메인에 따라 상이한 인증체계와 인증기술을 사용하고 있기 때문에, 이러한 기존 인증 체계와의 연동이나 통합을 손쉽게 수행할 수 있는 아키텍처의 설계 및 구현이 필요하다.

7) Tamper Resistance(탬퍼링 방지 기술)

DRM은 크게 서버군과 클라이언트군 소프트웨어로 나누어 구성된다. 서버는 이해관계가 동일한 집단 및 조직에 의해서 운영되기 때문에 그리 큰 문제점은 없다. 그러나 클라이언트 소프트웨어는 워낙 다양한 사용자들에 의해서 이용될 수 있도록 노출되어 있기 때문에 많은 위험 요소들을 안고 있으며, 그 중 가장 위협적인 부분이 악의적인 사용자에 의해서 소프트웨어의 구조 및 코드를 크래킹하는 것이다.

컴퓨터 기술이 발전함에 따라 소프트웨어 개발 기술도 발전하여 생산성 개선을 위해 Reverse Engineering Tool, Debugging Tool, reassembling Tool들이 많이 개발되었다. 그러나 이러한 툴들은 개발자의 생산성을 높이는 데에만 사용되는 것이 아니라 소프트웨어를 크래킹 하는 데에도 사용되고 있다. 따라서 Tamper Resistance는 이러한 크래킹 위협으로부터 소프트웨어를 안전하게 보호하는 것이 목적이라 할 수 있다.

Tamper Resistance는 DRM에 있어서 저작물의 안전한 배포 및 이용을 위해서 가장 중요한 기술 중 하나이다. 의도적으로 오작동하거나 소프트웨어 저작권 보호 장치 작동을 방해하는 행위를 방지하는 것으로, 리버스 엔지니어링이 어렵도록 하거나, 코드를 난독화 하는 방법 등이 있다.

위와 같이 소프트웨어의 복제 혹은 변경 자체를 어렵게 하는 기술적 보

호조치 외에 복제 혹은 변경한 불법 소프트웨어를 사용하여 저작권 침해가 기발생한 것을 전제로 그 사용자에 대한 형사고소 또는 민사상 손해배상 청구를 위해 증거수집을 위해 소프트웨어 내부에 크랙정보 수집 프로그램을 심는 것 역시 기술적 보호조치의 하나로 인정할 수 있을지 문제가 된다. 이에 대해 검토하기에 앞서 먼저 기술적 보호조치의 보호범위 및 기술적 보호조치의 무력화를 시도하는 크래킹 기술에 대해 살펴보고, 그와 같은 크랙정보 수집프로그램의 기술적 원리와 그에 대한 법적평가 등에 대해 검토한 후 후술하기로 한다.

마. 기술적 보호조치의 보호범위

이용통제조치 중 직접적 무력화 행위는 직접적으로 저작권을 침해한 경우를 의미하므로 저작권법이 이를 금지한다고 해석하는데 별다른 이론이 없다. 그러나 이용통제조치 중 간접적 무력화 행위나 접근통제조치의 경우는 이용자에게 새로운 제한을 가하는 결과로 되고 특히 접근통제조치에 대하여는 현재 새로운 권리로 창설되어야 한다는 논의가 미국을 중심으로 이루어지고 있다.

1) 미국에서의 관련 사례

Chamberlain Group, Inc. v. Skylink Technologies, Inc. 사건(381 F.3d 1178, Fed Cir. 2004))[32]에서 Chamberlain Group은 자신들이 가지고 있는 '차고문 개방장치에 쓰이는 다중 전송·단일 수신기에 대한 코딩 시스템' 관련 특허를 토대로, 캐나다에 있는 작은 회사인 Skylink Technologies에 대하여 그들이 판매하는 차고문 개방용 리모컨이 Chamberlain사의 차고문에서 작동하는 것은 자신들의 컴퓨터 프로그램에 대한 접근통제조치(access control)를 우회하여 무력화하는 것이라고 주장했다. 이에 대해 Skylink Technologies는 차고 소유자들이 원래의 리모컨을 분실한 경우에

32) https://www.eff.org/cases/chamberlain-group-inc-v-skylink-technologies-inc (최종 접속 2016. 10. 4.)

도 다른 회사의 리모컨을 구입하여 차고 문을 열수 있는 권리가 있다고 항변했다. 연방 순회법원은 'DMCA의 기술적 보호조치 조항이 추가적인 재산권을 부여하는 것이 아니고 재산권자에게 새로운 방어방법을 제공할 뿐이다'라고 판시하였다. 이는 저작권의 공정 이용 제한의 한계와의 조화를 모색하고 저작권의 오남용의 위험에 대한 경각심을 부여하며, 소비자 또는 경쟁업체에 대한 합리적인 기대의 범위를 넘어서서 저작권의 범위를 근본적으로 확장하지 않겠다는 입장, 즉 저작권에 의한 보호와 일정한 관계가 있는 기술적 보호조치만을 보호되는 것으로 한다는 입장을 명확히 한 것이다.

2) 우리나라에서의 관련 사례

소위 'PS2 모드칩' 사건(대법원 2006. 2. 24. 선고 2004도2743 판결)에서, 소니 엔터테인먼트사가 제작한 '플레이스테이션2' 라는 게임기 본체(이하 'PS2') 에서만 실행되는 게임 프로그램을 CD 등 매체에 저장해 판매하고 있는데 그 CD에는 '엑세스 코드'가 수록·저장되어 있고, PS2에는 '부트롬'이 내장되어 있어 엑세스 코드 없이 게임프로그램만 저장된 CD는 프로그램실행이 되지 않도록 설계되어 있음에도 PS2 콘솔을 분해하여 엑세스 코드가 수행하는 역할을 대신하는 부품인 모드칩을 PS2에 장착하여 주는 영업을 한 피고인에 대하여 구 컴퓨터프로그램보호법[33] 제30조 제2항 위반으로 약식명령이 청구되자, 피고인이 정식재판청구를 하였는데 1, 2심은 유죄판결을 선고하였다. 이에 대법원은 모드칩 장착행위가 기술적 보호조치의 무력화에 해당하는지에 관하여 엑세스 코드나 부트롬만으로 이 사건 게임프로그램의 물리적인 복제 자체를 막을 수는 없는 것이지만, 통상적인 장치나 프로그램만으로는 엑세스 코드의 복제가 불가능하여 설사 불법으로 게임프로그램을 복제한다 하더라도 PS2를 통한 프로그램의 실행은 할 수 없는 만큼, 엑세스 코드는 게임프로그램의 물리적인 복제를 막는 것과 동등한 효과가 있는 기술적 보호조치에 해당한다고 할 것이고, 따라서

33) 2009년 저작권법의 개정과 함께 컴퓨터프로그램보호법은 저작권법에 통합됨

피고인의 행위는 기술적 보호조치 무력화 행위에 해당한다고 판시하였다.

결국 접근통제조치의 무력화가 저작권으로 보호하려고 하는 보호범위를 침해하는 것과 직접 관련이 있는 경우인지 여부를 따져 직접관련이 있음을 전제로 유죄를 선고한 것이다.

기술적 보호조치에 대한 법적보호가 이루어지고 있음을 기화로 저작권보호와 아무 관련이 없는 기술적 보호조치에 대한 법적보호를 요구하는 경우 그 처벌가능성에 대해 부정적으로 봐야 한다. 일상생활기기에 컴퓨터 프로그램이 사용되는 것이 증가하고 있고 이 기기에 사용되는 '부품 시장'의 규모가 상당한 경우, 기기의 생산자는 자신이 판매하는 부품만 계속 기기에 사용되기를 희망하게 되고, 결국 기기 생산자는 경쟁자를 배제하기 위하여 경쟁자가 부품에 포함되어 있는 컴퓨터프로그램을 무력화하였다는 이유로 기술적 보호조치 규정의 위반을 주장하게 되는 부작용을 막기 위해서이다.

Ⅲ. 소프트웨어 크래킹 기술(기술적 보호조치 무력화 기술)

1. 프로그램 코드 역분석(Reverse Engineering)

리버스 엔지니어링이란 기존에 개발된 기술을 역으로 해석하여 보다 새롭고 진보적인 기술을 개발하기 위한 것으로 과거 공학후진국이던 우리나라가 외국의 기술을 획득하고 연구하기 위한 수단으로 주로 활용하던 것이다. 소프트웨어 분야에서는 오래된 소프트웨어를 개량하기 위해서나 상호 운영성 내지는 호환성을 분석하기 위해 리버스 엔지니어링 기술을 활용하기도 하지만, 저작권 보호를 위한 기술적 보호조치를 무력화 하는 수단으로 악용할 수도 있다.

리버스 엔지니어링 기술이 진보함에 따라 컴퓨터 소프트웨어에 대한 불법 조작 및 변조 등의 위협 또한 증가하게 되었고, 인터넷에 공개된 단순한 도구를 이용하여 누구나 쉽게 소프트웨어를 크래킹(Cracking) 할 수

있게 되었다.[34]

2. 소프트웨어 크래킹 기술의 폐해

대부분 소프트웨어는 사용자로부터 특정한 데이터 값을 입력받아 정상적인 데이터인지 여부를 검사한 후 결과를 사용자에게 보여주고, 입력된 데이터와 내부 데이터를 통해 처리하는 로직(process)에 따라 동작하는 형태의 일련의 과정을 취한다. 소프트웨어가 처리하는 이러한 루틴은 이를 모니터링하거나 리버스 엔지니어링 등의 방법을 통해 내부 비밀 데이터를 추출하거나, 처리되는 로직을 임의 조작하여 프로그램의 흐름을 초기 제작의도와 다르게 변경하여 사용할 수 있는 취약점을 가지고 있다.

소프트웨어를 위협하는 여러 가지 방식에는 위와 같이 지속적인 모니터링을 통해 데이터를 추출하는 것 외에도, 앞서 본 바와 같이 악의적인 목적을 가지고 소프트웨어를 임의로 조작하여 정품인증 코드가 아닌 아무 코드를 입력해도 정품으로 인증받게 하는 탬퍼링 기술, 저작사가 아닌 제3자가 불법으로 복제한 해적판의 재배포 등 여러 유형이 있다.

디지털 정보인 소프트웨어는 임의 조작을 통해 쉽게 원본과 동일한 복사본을 만들 수 있으며, 패키지 전체를 무작위로 재배포 할 수 있고, 컴퓨터 상에서 동작하는 어떤 소프트웨어라도 위와 같은 공격의 목표가 될 수 있다는 점에서 크래킹 기술의 폐해는 치명적이다.

3. 소프트웨어 크래킹 기술의 예

크래킹 기술은 소프트웨어가 사용하는 방어기술에 따라 달라질 수 있다. 등록키(Registration Key), 다중 일련번호(Multiple Serials)와 같은 단순한 등록번호를 사용할 경우, 등록번호를 비교하여 다음절차로의 이동을 차단

34) 김요식, 윤영태, 박상서, “윈도우 환경에서의 메모리 해킹 방지 시스템 연구”, 정보보증논문지 제5권 제3호(2005. 3.) 76면.

하는 코드상의 분기문(branch statement)[35]을 수정하거나 프로그래밍 언어로 작성된 코드를 보면서 취약점을 찾아내는 디버깅을 통해 하드코딩된 등록번호를 알아내거나 등록번호를 생성하는 알고리즘을 분석하여 등록번호만을 전문적으로 생성하는 프로그램[36]을 제작할 수 있다.

또한 디스크 등의 저장매체에서는 패커(Packer)에 의해 압축·암호화 되어 있는 코드도 컴퓨터 메모리상에서는 언패킹(unpacking)되어 실행된다는 취약점을 가지고 있어 외부공격자가 의도적으로 매뉴얼 언패킹을 이용하여 패커 기능을 무력화 시킬 수 있다.

패킹되어 있는 프로그램이 메모리에서는 언팩되어 실행되는 것을 이용해서, 디버깅을 통해 패킹되어 있는 프로그램 코드를 읽고 반복되는 코드를 공격해서 의도적인 오작동을 유발할 수 있도록 일련의 명령을 만들어 영구적으로 패치하는 기술(프로세스 패치), Win 32 API를 사용하여 로더라는 별도의 프로그램을 제작하여 대상 프로그램이 가지는 메모리 영역의 권한과 코드를 수정하는 패치 기술 등도 여전히 각종 소프트웨어에 적용 가능하다.

소프트웨어의 불법적인 복사를 방지하기 위한 기술로 하드웨어를 이용하는 경우, 즉 컴퓨터의 I/O 포트에 USB 등 작은 하드웨어를 부속시키는 동글(Dongle)에 대해서는 위조된 드라이버(Driver)를 제작하거나 별도의 에뮬레이터(Emulator)[37]를 이용하여 동글 없이도 소프트웨어를 동작할 수 있는 크래킹 방법이 사용되고 있다.

4. 크랙정보 수집 프로그램의 문제점

가. 크랙정보 수집프로그램의 원리

크랙정보를 수집하는 다양한 프로그램 중 컴퓨터 지원설계(Computer

35) 프로그램 중간에 어떠한 조건에 따라 다른 명령을 실행하게 하는 문법
36) key-generation의 줄임말로 '키젠'이라고도 한다.
37) 어떤 하드웨어나 소프트웨어의 기능을 다른 종류의 하드웨어나 소프트웨어로 모방하여 실현시키기 위한 장치나 프로그램

Aided Design, CAD) 분야의 고가형 소프트웨어 등에 주로 사용되는 V.I.LABS 사의 'Code Amor'[38]라는 프로그램의 예를 통해서 본다.

Code Amor는 독립적으로 설치되는 소프트웨어가 아니라, 판매되는 소프트웨어의 응용프로그램에 내장되는 일종의 '기능성 함수'로서, 평상시에는 비활성화 되어 있다가 응용프로그램이 부당하게 변경되거나 하는 침해행위가 감지되어 정품이 아닌 불법 복제한 소프트웨어를 사용한다고 의심될 만한 상황에서만 활성화된다.

또한 Code Amor는 스파이웨어[39]처럼 컴퓨터가 켜져 있는 동안 항상 작동하면서 사용자의 정보를 추적하며 수집하는 것은 아니지만, 불법소프트웨어 사용을 의심할만한 상황에서는 사용자의 IP주소, MAC 주소, 도메인 등 호스트 환경의 특정 자료를 수집하고 이를 소프트웨어 판매자의 네트워크에 설정된 하나 이상의 Web gateway[40]로 전달한다.

구체적인 예로 미국 PTC사의 3차원 CAD 소프트웨어 'Creo' 프로그램은 정품 소프트웨어의 라이선스 파일 안에 위 Code Amor를 삽입하여, 사용자가 허용되지 않은 라이선스 키를 입력하거나 기술적 보호조치가 무력화된 소프트웨어를 사용하는 경우 그 정보가 PTC사의 서버로 전송되게 한다.

위 정보를 받은 PTC사에서는 크랙정보중 IP 주소를 IP 주소 검색사이트 'Who is'를 통해 검색하여 해당 IP 주소가 국내의 특정 ISP(internet service provider)가 할당받은 주소임과 해당 프로그램을 사용하는 기업체의 사명, 사업소 소재지 등을 알아내고, 해당 기업체에는 PTC사로부터 소프트웨어를 구입하거나 라이선스 계약을 체결한 사실이 없음을 확인하고 이를 바탕으로 저작권법위반을 이유로 수사기관에 형사고소 할 수 있다.

---

38) http://www.vilabs.com/code-confidential-post/thinking-differently-about-software-piracy-comments-on-codearmor-intelligence(2016. 9. 27. 확인)

39) 스파이(spy)와 소프트웨어의 합성어로 다른 사람의 컴퓨터에 몰래 숨어들어가 있다가 중요한 개인정보를 빼가는 프로그램을 지칭한다

40) 클라이언트/서버 모형을 사용하여 재정 분석, 제조 공정, 인간 자원 관리 및 기타 비즈니스 처리를 위한 데이터를 저장, 검색, 분석, 처리하는 포괄적인 비즈니스 애플리케이션인 R/3 애플리케이션에 접속할 수 있는 인터넷 거래 서버(Internet Transaction Server, ITS)의 한 요소. Web gateway가 ITS와 웹 서버간의 접속을 설정하고 사용자 요구사항을 Application gatewa(Agate)에 보내면 R/3 애플리케이션과 인터넷 간의 데이터를 처리한다.

위 고소장이 접수됨으로써 성명불상자의 'Creo'프로그램 불법복제 사용 혐의가 형사사건으로 입건되면 담당 검사는 고소인측에서 제출한 크랙정보 수집 프로그램을 통한 피혐의자의 IP 주소 등의 정보가 유일한 소명자료일 때 이를 토대로 수사를 진전시켜나가기 위해 해당 IP 주소를 사용하는 기업체의 사무실 컴퓨터, 서버 등에 대한 압수수색을 진행하기 위해 영장을 청구할 것인지 여부를 결정하게 된다.

나. 크랙정보 수집 동의의 적법성

1) 사용자의 동의 여부

크랙정보 수집 프로그램을 통해 불법사용자의 존재를 파악하고 형사고소를 한 저작권자의 입장에서는 해당 프로그램을 설치할 당시, 소프트웨어의 불법 복제 사용자에 대하여 크랙정보를 수집할 것임을 고지하였고, 그에 동의하는 경우 '동의'버튼을 클릭하여야만 프로그램이 설치될 수 있었으므로 해당 프로그램의 사용자들은 모두 위와 같은 크랙정보 수집 및 정보제공에 동의한 것이라고 주장한다.

그러나 위와 같은 소위 클릭랩 라이선스 계약의 유효성 여부에 대해서는 많은 논의가 있다.

2) 소프트웨어 이용허락계약의 유형

소프트웨어는 유통의 대상이 프로그램 저작권인지 프로그램 저작물인지에 따라 계약의 형태가 달라진다.[41]

유통의 대상이 프로그램 저작권이라면 프로그램 저작권을 양도하여 이익을 얻는 형태가 된다. 이때의 권리는 완전히 무형의 것으로 실체가 없으며, 저작권을 권리의 다발로서 전체 양도할 수도 있고 일부만 양도하는 것도 가능하다. 사용자의 필요에 맞춘 주문제작형 응용 소프트웨어를 개발하고 사용자에게 저작권을 양도하는 경우가 있는가 하면, 이미 개발된

41) 김현숙, "멀티유저 PC를 중심으로 살펴본 소프트웨어 이용허락계약 체결과 저작권 침해 문제", 「안암법학」 43권 (2014), 885면.

패키지형 소프트웨어를 인수, 합병 등의 이유로 이에 관한 모든 권리를 양도하는 경우 등이 있다.

반면 프로그램 저작물을 유통의 대상으로 본다면 이 역시 무형의 것이기는 하지만 디지털 정보나 파일이라는 저작물의 사용을 허락하는 이용허락 형태의 거래가 된다. 이때는 권리 자체를 양도하는 것이 아니라 그 저작물을 일정 수량 혹은 일정 기간 이용할 수 있도록 하는 것일 뿐이다. 동일한 저작물을 다수의 사용자에게 제공하는 경우로, 패키지 소프트웨어의 거래도 이에 해당한다.

이러한 패키지 소프트웨어에 대한 이용허락의 대표적인 방법은 박스를 개봉하면 계약이 성립된다고 보는 쉬링크랩(Shrink-wrap)계약, 혹은 이용에 동의한다는 버튼을 클릭하면 계약이 성립된다고 보는 클릭랩(Click-wrap) 계약이다.

3) 클릭랩 계약의 의의

1970년대에는 하드웨어가 거액에 거래되었기 때문에 소프트웨어는 그에 따라가는 번들로써 제공되는 경우가 대부분이었으나, 1980년대 들어 컴퓨터의 생산가가 낮아지며 개인용 컴퓨터, 즉 PC의 대량보급이 이루어졌다. 이에 따라 소프트웨어 계약도 급속히 증가하게 되었다. 이때마다 판매자와 구매자 사이의 별도의 협상이나 계약을 체결하는 것은 현실적으로 불가능하게 되었기에 소프트웨어 판매자들은 소위 쉬링크랩 방식의 계약을 고안해 내었다. 쉬링크랩 방식은 소프트웨어의 포장을 뜯어서 그것을 사용할 경우 포장박스 또는 비닐포장 안에 포함되어 있는 라이선스 약관에 동의하는 것을 의미한다는 문구를 겉면에 인쇄하여 붙여 놓는 형태의 약관 제시방법이다.[42]

내용도 어려운데다 글씨도 작고 복잡한 그 많은 조항에 대해 단순히 포장을 뜯거나 화면의 동의 버튼을 클릭하는 것만으로 완전한 승낙이 이뤄졌다고 보아야 하는지에 대해서 과거에는 계약의 유효성을 부인하는 판결

42) 최광준, “소프트웨어계약과 라이선스 약관의 유효성”, 「경희법학」 제44권 제1호, 150면.

들도 있었으나[43], 1990년대 이르러서는 계약의 유효성이 인정되기 시작하였다.[44]

클릭랩 라이선스 계약이란 쉬링크랩 이용계약에서 파생된 것으로, 박스 등에 계약조건이 있는 것이 아니라 소프트웨어를 설치하는 과정에서 컴퓨터 화면에 사용허락에 관한 계약조건을 명시하고 이에 동의한다는 버튼을 클릭하면 계약 조건 아래 사용 허락 계약이 체결되는 방식이다.

쉬링크랩이나 클릭랩 계약을 통해 체결되는 계약의 명칭은 최종 사용허락계약, 최종 이용자 이용 약관, 소프트웨어 사용권 계약서, 소프트웨어 라이선스, 최종 사용자 사용권 계약 등 다양한 이름으로 불리는데, 일반적으로는 '최종 사용자 라이선스 동의(EULA: End User License Agreement)'로 통용된다. 오늘날은 소프트웨어 저작권자가 박스형 소프트웨어를 출시하기보다 설치 CD만 제공하거나 혹은 온라인을 통해 설치 파일만 제공하는 추세이므로 쉬링크랩 계약보다 클릭랩 계약이 더 일반적이다.

미국에서는 쉬링크랩 계약의 유효성을 인정하는 ProCD 판결 이후, 그 판결을 인용하며 Specht v. Netscape Communications Corp. 판결[45]을 통해 클립랩 계약의 유효성 또한 인정하고 있다.

앞서 예로 든 PTC사의 'Creo'프로그램의 경우, 'PTC customer agreement'에서 "Please read the terms and conditions of this agreement carefully before accepting this agreement. By clicking on the 'I accept' button below or by installing, accesing, or using any

43) Step-Saver Data Sys., Inc. v. Wyse Technology, 939 F.2d 91 (3d Cir. 1991); Vault Corp. v Quaid Software Ltd. 847 F.2d 255 (5th Cir. 1988).

44) ProCD Inc. v. Zeidenberg 86 F.3d 1447 (7th Cir. 1996); Caspi v. The Microsoft Network, 323 N.J. Super. 118, 732 A.2d 528 (1999); i.Lan Systems, Inc. v. Netscout Service Level Corp., 183 F.Supp.2d 328 (D. Mass. 2002).

45) Specht v. Netscape Communications Corp.(2001), 150 F. Supp. 2d. 585. : Netscape사는 웹사이트에서 여러 프로그램을 다운로드하도록 게시하고 있었는데, 그 중의 하나가 문제의 통신 프로그램이었다. 이것은 무상으로 다운받을 수 있도록 되어 있었는데, 프로그램을 다운받아 개인용 컴퓨터에 설치를 하는 과정에서 스크롤이 가능한 라이선스 약관이 게시되고 이 약관에 동한다는 의사를 "YES" 버튼을 눌러 확인시켜 주지 않는 한, 설치프로그램이 더 이상 진행되지 못하도록 장치가 되어 있었다. 법원은 "I accept" "I agree" 등으로 표시되어 있는 버튼을 클릭함으로써 성립하는 여러 가지의 유사한 계약들을 열거하면서 클릭을 통해 약관내용에 "동의"한다는 의사를 표명한 것으로 해석하고, 클랙랩 방식에 의한 약관의 구속력을 인정하였다.

software or documentation from PTC, **customer hereby agrees** to be bound by this agreement and represents that it is authorizes to do so." 라는 문구를 통해 클릭랩 계약을 체결하고 있다. 위 문구는 프로그램을 최초 설치할 때, 영문으로 모니터 화면에 제시되며, 동의함 버튼을 클릭해야만 프로그램이 설치되고 이를 사용할 수 있다.

클릭랩 라이선스 계약의 유효성은 미국은 UCITA §102(44), 일본은 経済産業省, 電子商取引及び情報財取引等に關する準則 (2014. 8), iii. 2～iii. 3頁, 우리나라는 약관규제법에 의해 그 근거를 찾을 수 있는 것으로 본다.

4) 클릭랩 계약의 주요내용 및 목적[46]

클릭랩 약정은 인터넷을 통해 제품과 서비스를 판매하는 기업에게 그 제품과 서비스에서 발생하는 지적재산권에 의해 중요한 보호를 제공한다. 이와 함께 클릭랩 약정은 묵시적 보증에 대한 면책, 제품구매와 관련된 보상 책임의 제한, 분쟁 해결을 위한 준거법과 법정지의 명시, 사용권의 제한, 비저작권 제품의 보호, 소프트웨어 프로그램의 역분석(reverse engineering, decompilation)의 금지에 관한 사항들을 주로 담고 있다.

소프트웨어에 대한 클릭랩 라이선스 약정은 저작권법상의 최초 판매 법리(First Sale Doctrine)의 적용을 피하려는 의도에서 활용된다. 최초 판매의 법리는 저작물의 원작품이나 그 복제물이 배포권자의 허락을 받아 판매의 방법으로 제공된 경우에는 이를 계속 배포할 수 있다는 것으로 '권리소진의 원칙', '권리소모이론'이라고도 한다. 즉 저작물의 복제본 구입자가 그 복제본을 양도하거나 판매하는 것을 허여한다는 내용이다. 최초 판매의 법리가 상거래 시장에서 소프트웨어의 양도에 적용된다면, 원본 구입자가 다른 사람에게 복제본을 판매하거나 빌려주는 것이 가능하여, 소프트웨어 개발자들은 많은 손해를 보게 될 것이다. 그러나 소프트웨어에 대한 라이선스 약정을 클릭랩 방식으로 간단히 체결함으로써 소유권 양도

46) 이충열, "클릭랩 약정의 효력요건에 관한 연구-미국의 입법과 판례를 중심으로-", 「국제상학」 제20권 제3호, 26면.

가 금지되어, 공급자는 수입을 극대화하고 소프트웨어에 대한 저작권 침해를 피하며, 저작권자가 타인의 저작권 침해 행위로부터 저작권을 주장할 필요가 없어진다.

5) 클릭랩 계약의 효력요건

클릭랩 계약이 유효하기 위해서는 몇 가지 요건을 충족해야 할 것이다. 우선 조건 검토의 기회와 관련해서 사용자에게 먼저 약정조건을 보여 주지 않고 동의하도록 해서는 안된다. 약정 조건은 자동적으로 보이거나, 사용자가 클릭할 때 쉽게 찾을 수 있는 아이콘이나 하이퍼링크를 보여야 한다. 동의 버튼은 약정조건의 끝에 위치시켜, 사용자가 약정조건을 다 통과한 뒤에 동의하도록 하여야 한다. 최근의 판례와 미연방거래위원회(FTC) 가이드라인을 볼 때, 사용자가 동의하기 전에 제시된 약정 조건을 검토하도록 요구하고 있지 않을 경우, 클릭랩 약정의 효력을 확보하기가 어렵다는 점을 알 수 있다 또한 사용자는 약정조건에 동의하지 않고서는 웹사이트, 소프트웨어, 컴퓨터 정보, 재산 또는 서비스에 접속하거나 권리를 가져서는 안된다. 약정 조건은 사용자가 약정이 적용되는 상품을 획득하기 전에 제시되어 동의를 받아야 한다. 또한 프로그램 구매 또는 설치 절차를 진행하기 전에 충분한 검토 기회를 제공받아야 한다. 자신에게 맞는 속도로 약정 조건을 읽을 수 있어야 하고, 조건을 한번 읽어본 후에도 지속적으로 웹사이트 상에서 반복 검토가 가능해야 한다. 또한 조건은 형식과 내용면에서 사용언어, 가시성, 명료하고 읽기 쉬운 글자체 등에 관한 관련법률(소비자보호법, UCC, 결제 및 금융관계규정 등)과 합치해야 하며, 저작권자가 사용자에게 제공한 다른 정보와 상충되지 않아야 하며, 의미의 모호성이 없어야 한다. 또한 동의나 거절에 대한 명확한 용어를 사용하고, 동의나 거절 결과에 대하여도 명확히 고지해야 하며, 동의한 사용자가 오류를 정정할 기회를 제공해야 하고, 동의를 입증할 수 있는 기록을 유지해야 한다.[47]

47) 이충열, “클릭랩 약정의 효력요건에 관한 연구-미국의 입법과 판례를 중심으로-”. 「국제상

6) 소프트웨어 불법복제 사용에 적용가부

위와 같은 요건을 구비하여 유효한 클릭랩 계약이라고 인정할 수 있다고 해도, 이를 소프트웨어 불법 사용자에게도 동일하게 적용할 수 있을 것인가 하는 의문이 남는다. 실제로 불법복제 사용자는 소프트웨어를 구매하는 계약을 체결할 의사가 없고, 클릭랩 약정에도 불구하고, 오히려 저작권자의 저작권을 침해하는 행위를 예정하고 있거나, 이미 동의함 버튼을 클릭하는 행위자체가 불법복제한 소프트웨어 설치행위의 한 과정으로 저작권을 침해하는 행위를 하고 있는 중임에도 '동의함' 버튼을 누름으로 사용자가 약관에 동의하는 것으로 의제되며, 저작권자의 저작권을 침해하지 않는다는 계약 당사자의 의무를 부담하게 되는 아이러니한 상황이 발생한다. 불법 복제 사용자가 정당한 반대급부를 지급하고 소프트웨어 사용권한을 취득하는 계약을 체결할 의사는 없다 하여도, 적어도 해당 소프트웨어의 내용, 기능, 효과 등에 대해 인지하고 자기 책임하에 이를 자신이 사용하는 PC에 설치할 것이고 그에 수반하여 프로그램 설치 및 이용을 위하여 준수해야 하는 최소한의 프로토콜 매뉴얼을 따르겠다는 의사를 표명한 것으로 일종의 비전형계약이 체결된 것으로 볼 수 있다. 그러나 위와 같은 동의가 당사자 간의 계약상의 권리의무를 발생시키는 사법(私法)상의 계약으로 유효하다고 할지라도 이를 바탕으로 형사상의 처벌을 전제로 하는 형사소송의 증거로 제공하는데 까지 유효한 동의를 한 것이라고 볼 수 있을지는 별개의 문제로 판단해야 한다.

특히 위에서 예로 든 'Creo'프로그램의 예에서 보면, 위 동의함 버튼 클릭에 대한 설명에 이어 아래와 같은 문구로 불법복제본을 사용할 시에는 사용자에 대한 데이터를 PTC에 전달한다는 취지를 표시한다.[48]

If customer did not obtain the licensed product from PTC directly, from an authorized PTC distributor or reseller or from the PTC

학」 제20권 제3호, 35~42면.

48) PTC Clickwrap Customer Agreement - Rev. 10/10

online store(at www.ptc.com), customer is using an illegally obtained unlicensed version of the applicable licensed product. PTC regards software piracy as the crime it is and pursues(both civilly and criminally) those who take part in these activities. as part of these efforts, **PTC utilizes data monitoring and scouring technologies to obtainand transmit to PTC data on users of illegal copies of Licensed Products.** This data collection is not performed on users of legally licensed units of licensed products. If customer is using an illegal copy of software and does not consent to the collection and transmission(including to the United states) of such data, Cease using the illegal version and contact PTC to obtain a legally licensed copy.

그런데 위와 같은 설명 내지 경고의 문구는 영문으로만 화면에 나타날 뿐이어서, 비영어권 국가 혹은 국내에서 이를 설치하여 사용하는 당사자가 그 내용을 읽고 이해한 후 진정한 동의의 의사로 'I agree' 버튼을 클릭하였을 것이라고 기대하기 어렵다.

비단 위 문구가 영문으로 제시된다는 사용언어에 관한 측면 외에도 위와 같은 프로그램 설치과정에서 사용자는 프로그램이 유효하게 작동할 수 있도록 컴퓨터에 설치하는 것에 주된 관심이 있어, 이를 필수적이고 형식적인 절차로 이해하고 프로그램의 기능, 설치방법 및 위치, 작동요령, 오작동시의 제작자의 면책 등의 요소에 대해 동의하는 의사로 클릭하였을 것이지, 이때의 동의를 자신에 대한 재산상, 신체상의 극단적인 불이익인 형사처벌에 쓰이는 것까지를 동의한 것으로 보고, 형사처벌을 전제로 하는 형사소송절차중 강제수사의 하나인 영장에 의한 압수수색의 적법성의 근거를 당사자의 동의라고 주장하기는 어렵다. 헌법 제12조 제2항에서 '모든 국민은 형사상 자기에게 불리한 진술을 강요당하지 아니한다'라고 하여 자기부죄금지원칙, 진술거부권을 헌법상의 권리로 인정하는 취지를 고려하면 이는 더욱 분명해진다. 또한 사용자의 구체적인 동의 없는 사인의

포괄, 일반적인 크랙정보 수집행위가 위법하다면, 사용자의 사전적인 동의로 그 위법성이 조각될 것인지 즉, 사용자의 IP 주소 등에 대한 보호가 스스로 처분할 수 있는 법익인지 여부도 문제된다.

Ⅳ. 크랙정보 수집프로그램을 통해 획득한 IP 주소 등의 문제점

1. IP 주소의 개인정보성 여부

가. IP 주소의 의의

IP 주소란 인터넷에 연결된 컴퓨터 등에 부여되는 고유의 식별 주소를 의미한다. 4개의 10진수 형태로 구성되며, 각 10진수는 8자리 2진수를 의미하는 것으로 결국 IP 주소는 32비트로 구성된다. IP 주소의 유형에는 접속할 때 마다 할당된 주소가 달라지는 유동 IP(dynamic IP)와 고정된 주소를 갖는 고정 IP(static IP)가 있다.

IP 주소는 네트워크 주소와 호스트 주소로 나뉘는데, 네트워크 주소로는 기기가 속해있는 네트워크를 식별할 수 있고, 호스트 주소는 해당 네트워크에서 그 기기를 식별하는데 사용한다. 한 네트워크에 포함된 모든 기기들은 같은 네트워크 주소를 갖고 있어야 하지만, 한 네트워크 내에 같은 호스트 주소를 갖는 여러 기기가 있으면 안된다.

이용자들이 웹을 검색하거나 이메일을 보내는 경우, 이용자가 접속하는 사이트는 이용자의 IP 주소를 비롯한 일정한 정보를 수집한다. IP 주소는 특정한 시간에 특정 웹사이트에 접속한 컴퓨터를 나타내게 되고, 인터넷 이용자의 컴퓨터를 통한 인터넷상 행위는 웹사이트에 기록된다.

따라서 IP 주소는 컴퓨터뿐만 아니라 이용자의 인터넷상 행위와도 연결될 수 있다. 그러나 컴퓨터가 접속한 사이트는 컴퓨터 내지 그 이용자가 누구인지를 식별할 수 없으며, ISP만이 이용자와 IP 주소를 비교할 수 있다.[49]

---

49) 이대희, “개인정보 개념의 해석 및 범위에 관한 연구”, 「고려법학」 제79호(2015. 12.), 181면.

이러한 IP 주소를 개인을 식별할 수 있는 개인정보라고 볼 것인가 여부가 문제이다.

나. 비교법적 검토

미국의 의료정보보호법인 Health Insurance Portability and Accountability Act(HIPAA)는 명시적으로 IP 주소를 식별정보로 분류하고 있고, 유럽 각국 대표로 구성된 유럽연합의 개인정보 관련 자문기구인 'Article 29 Working Party'는 2008년, 유동 IP 주소라도 적절한 조치(reasonable means)를 취하면 개인을 알아낼 수 있으므로, IP 주소는 개인식별정보라고 결론 내렸다.[50] 즉 인터넷접속제공자, 각 지역 네트워크 관리자, ISP는 인터넷 이용자에게 IP 주소를 부여하고, 날짜, 시간, 기간 및 유동 IP 주소를 체계적으로 기록하고 이러한 기록을 서버에 저장한다. 이러한 기록이 이용자의 IP 주소와 연결될 수 있다면, 곧 이러한 기록과 이용자의 IP 주소를 연결시키는 것이 가능하다면, IP 주소는 개인정보에 해당한다는 것이다. 이 결론은 구속력은 없지만 유럽의 행정기관 및 유럽연합에 설치된 유럽사법재판소는 위 Article 29 Working Party의 결론에 따라 IP 주소의 식별정보성을 인정하는 편이다.[51]

그러나 유럽 각국 법원의 판례는 IP 주소의 식별정보성을 인정하는 판례와 그렇지 않은 판례로 나뉘고 있다. 2008년 9월경, 독일 뮌헨 법원은 IP 주소를 알아냈다고 하더라도 이를 통해 개인을 알아내는 과정에 불법이 매개될 수밖에 없으므로 IP 주소는 개인정보라고 할 수 없다고 판시했고[52], 2010년 4월경, 아일랜드 고등법원(High Court)은 EMI Records v. Eircom Ltd 사건에서 저작권 단속을 위하여 음반회사가 수집한 IP 주소

---

50) Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 16-17 (01248/07/EN WP 136, June 20, 2007)

51) 김경환, "IP주소는 개인식별정보인가", 인터넷 신문 「보안뉴스」 2013. 3. 4.자 기사 http://www.boannews.com/media/view.asp?idx=35078&kind=1

52) Jeremy M. Mittman, German Court Rules that IP Addresses Are Not Personal Data, http://privacylaw.proskauer.com/2008/10/articles/european-union/german-court-rules-that-ip-addresses-are-not-personal-data

정보는 개인정보에 해당하지 않는다고 판시했으며 2009년 1월경, 프랑스의 대법원(Supreme Court)는 SACEM[53] v. Cyrille Saminadin 사건[54]에서, 작곡자, 저자, 음반제작자 협회가 예술가를 대신해서 지적재산권을 보호하기 위해 불법복제 사용자에 대한 조사를 실시하고, 무단으로 P2P사이트를 통해 음악 등을 공유한 저작권 침해자의 IP 주소를 조사하고 어떤 ISP가 해당 IP 주소를 제공하는지 확인하여 경찰에 신고한 사안에서, 범죄자가 사용하는 ISP를 찾기 위해 IP 주소를 조사하는 것은 해당 범죄에 관련된 개인정보의 자동처리절차와 관련이 없으므로 IP 주소는 개인정보가 아니라는 취지로 판시했다.

한편, 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)의 2010년도 발간자료에 따르면, IP 주소, MAC 주소 또는 지속적으로 특정 개인 등과 연결되어 있는 고정 주소는 식별정보로 볼 수 있다고 하였음에도, 미국 법원은 대체로 IP 주소가 식별정보가 아니라고 판시하고 있다. 예컨대 2011년 5월경, 일리노이 지방법원은 VPR Internationale v. Does 1-1017 사건[55]에서 하나의 IP가 한 사람과만 관련이 있다고 단정할 수 없으므로 IP 주소는 개인의 식별정보에 해당하지 않는다고 판시했고 2009년 7월경, 워싱턴 서부지방법원은 Johnson v. Microsoft Corp. 사건에서 IP 주소는 식별정보를 구성하지 않는다고 보았다. 반면 뉴저지 대법원은 2008년경, State v Reid 사건에서 IP 주소라고 하여 프라이버시 보호 대상에서 벗어나는 것은 아니라고 판시한 바 있다.

한편 아시아에서 홍콩 개인정보 당국은 2007년경, IP 주소는 특정 기계나 디바이스에 할당된 것이지, 개인에 관한 정보가 아니므로, 식별정보로 볼 수 없다는 결론을 내린바 있다.[56]

다. 우리나라의 경우

---

53) The Society of Composers, Authors and Music Publishers
54) http://www.out-law.com/page-10802
55) http://www.getflexner.com/posts/vpr-internationale-v-does-1-1017/
56) http://privacyblog.naver.com/80184674073, 네이버 개인정보보호위원회 공식 블로그

우리나라에서는 2011년 11월경, 접속 IP 주소를 수집하는 모바일 애플리케이션을 만들어 배포한 사건에서, 서울중앙지방검찰청은 '같은 AP(Access Point) 사용대역 내에서는 복수의 모바일 기기 이용자가 동일 IP 주소로 접속하고 있으며, 유동 IP 주소의 경우에는 시간대별로 IP 주소가 변동될 수 있으므로, 본 사안에서 IP 주소는 개인정보로 볼 수 없다'는 취지의 결정을 내린 바 있다.

최근에는 IP 주소의 식별정보성에 대한 결론은 상황에 따라 달라질 수 있다고 보는 의견이 많다.

기본적으로 IP 주소는 디바이스나 기계에 관한 정보이지 PC 이용자 등에 대한 정보는 아니며, 대부분의 PC나 모바일 기기가 유동 IP 주소를 할당받아 사용하는 상황에서 IP 주소를 알았다고 하여 사용자를 특정할 수 있는 것은 아니고 하나의 PC를 여러 사람이 사용하는 경우도 역시 IP 주소를 파악했다고 하여 특정 개인과 연관시키기 곤란하기 때문에, 기본적으로 IP 주소는 식별정보가 아니라는 것이다.

다만 고정 IP를 사용하는 PC가 있고 그 PC를 특정 개인이 또는 각자의 아이디로 특정할 수 있는 소규모의 집단이 지속적으로 사용했다면, 이 경우에는 IP 주소를 식별정보로 볼 수 있을 것이다. 영국의 ICO(Information Commissioner's Office)도 같은 입장을 취하고 있다.

라. 소결

크랙정보 수집 프로그램을 이용하여 불법 복제 소프트웨어 사용자의 IP를 수집해 수사기관에 고소한 저작권자의 입장에서는 IP 주소가 개인정보가 아니라는 가정하에 이를 정보주체의 동의 없이 수집해도 법위반이 되지 않는다고 주장하거나, 혹은 IP 주소가 개인정보에 해당한다고 보더라도, 위에서 본 클릭랩 라이선스 계약을 근거로 정보주체의 동의를 얻은 경우에 해당하므로 개인정보보호법 제15조 제1항 제1호[57]에 의해 법률상

57) 개인정보보호법 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우

근거가 있다고 주장한다.

그러나 앞서 본바와 같이 IP 주소가 개인정보로 볼 수 있을지 여부가 명확하지 않을 뿐 아니라, 설사 이를 개인정보로 볼 수 있다 하여도, 클릭랩 라이선스 계약에서 프로그램 설치 및 사용에 관한 동의를 개인정보 수집 및 활용에 대한 처분행위로서의 동의로 간주하기 어렵고, 개인정보보보호법 이전에 IP 주소가 통신비밀보호법상의 통신사실 확인자료에 해당한다면 특별법으로서 통신비밀보호법의 적용을 먼저 검토해야 할 것이다.

2. IP 주소의 통신사실 확인자료성

가. 통신자료와 통신사실 확인자료

그동안 통신의 비밀과 관련한 논의는 주로 통신비밀보호법상의 감청 등 통신제한조치를 대상으로 이루어졌다. 그러나 2000년대 중반 이후 정보통신환경이 확대되고, 스마트폰의 보급이 보편화된 이후 통신자료는 개인정보 보호뿐만 아니라 사생활 보호 차원에서도 중요한 자료가 되었고, 통신자료 자체가 개인의 인권보장 차원에서 소홀히 할 수 없는 의미를 가지게 되었으며, 수사에서 차지하는 비중 또한 커졌다.[58)]

현행법상 수사기관이 전기통신사업자에게 이용자의 통신자료를 요청할 수 있는 형태는 2가지로 구분된다. 하나는 전기통신사업법상의 '통신자료'이고, 나머지 하나는 통신비밀보호법상의 '통신사실 확인자료'이다. 과거 구 전기통신사업법 제54조 제3항[59)]은 현재와 같이 통신자료와 통신사실

---

2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

58) 권양섭, "범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안", 「한국법학회-법학연구 제59집」,(2015), 399면.

확인자료를 구분하지 않고, 전기통신업무에 관한 서류로 포괄적으로 규정하고 있었기에 양 자료는 현재와 같은 구분 없이 모두 전기통신사업법에 의해 법원의 허가 없이 수사기관의 필요에 따라 전기통신사업자에게 요청할 수 있었다.

그러나 2001년에 통신비밀 보호를 강화하기 위하여 전기통신사업법에 의한 통신자료제공을 개인신상과 관련된 정보로 제한하고, 통신이용사실과 관련된 내용은 통신비밀보호법에 의해 요청하도록 관련법이 개정되었다.

(1) 전기통신사업법상의 통신자료는 '이용자의 인적사항과 관련된 성명, 주민번호, 주소, 전화번호, 아이디(이용자 식별번호), 가입일 또는 해지일' 등의 정보이고, (2) 「통신비밀보호법」상의 통신사실 확인자료[60]란 ① 가입자의 전기통신일시, ② 전기통신개시·종료시간, ③ 발·착신 통신번호 등 상대방의 가입자번호, ④ 사용도수, ⑤ 컴퓨터통신 또는 인터넷의 사용자가 전기통신 역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, ⑥ 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, ⑦ 컴퓨터 통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적 자료를 말한다.

나. 비교법적 검토

1) 통신자료와 통신사실 확인자료 구별여부

미국은 통신자료와 통신사실 확인자료를 구분하여 규정하고 있지 않다. 통신과 관련한 고객의 인적 사항 등 통신자료제공과 관련하여 당사자의 동의가 없는 이상 법원 또는 대배심의 명령장이 필요한 것이 원칙이다.[61]

---

59) 구 전기통신사업법 제54조 제3항 전기통신사업자 또는 전기통신사업자로부터 전기통신업무의 일부를 수탁하여 취급하는 자는 수사상 필요에 의하여 관계기관으로부터 전기통신업무에 관한 서류의 열람이나 제출을 서면으로 요구받은 때에는 이에 응할 수 있다.

60) 통신비밀보호법 제2조 제11호

61) 이성기, "통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차에 관한 비교법적 연구: 미국, 영국, 독일, 프랑스, 일본의 제도를 중심으로", 「한국법정책학회 법과 정책연구」 제14권 제1호(2014.3.), 47면.

영국 수사권한규제법(RIPA, Regulation of Investigatory Powers Act 2000)은 미국과 같이 통신사실과 통신사실 확인자료를 별도로 구분하여 규정하고 있지 않다. 위 법률에 의해 통신자료의 제공은 영장주의가 적용되지 않고 수사권한규제법에서 통신사업자의 정보제공의무를 규정하고 관련기관의 개별 법령에 별도로 규정하는 방식을 취하고 있어, 기관의 일정 간부가 이를 허가하면 요청서를 근거로 자료를 제공하고 있다.[62] 이에 반해 독일은 형사소송법에서 '교신데이터'의 수집에 대한 일반적인 권한을 규정하고 있는데 그 구체적인 대상은 독일정보통신법 제96조에 명시되어 있는 ① 번호 또는 전기통신참가자 혹은 단말기기의 식별번호, 개인인증코드, 고객카드를 사용할 경우는 고객카드번호, 모바일 연결기기를 사용할 경우는 위치정보, ② 요금이 전송되는 데이터의 양에 의존하는 경우 통신시간과 날짜에 따른 각각의 통화의 시작과 끝, ③ 사용자에 의해 요구되는 통신서비스, ④ 망 연결의 종료시점, 그것의 날짜와 시간을 기준으로 한 그것의 시작과 끝 그리고 요금이 전송된 데이터 양에 의존할 경우 전송된 데이터의 양, ⑤ 전기통신의 구축과 유지, 요금정산을 위한 교신데이트 등으로 우리나라 통신비밀보호법상의 '통신사실 확인자료'와 대체로 일치한다. 또한 독일정보통신법(TKG) 제3조 제30호에서는 통신자료를 통신정보서비스에 대한 계약관계의 성립, 실질적인 형성, 변경, 해지와 관련된 계약 당사자에 대한 일체의 정보라고 정의하고 있다. 이는 우리나라 '통신자료'와 대체로 일치한다.[63]

2) 통신자료 제공 요건과 절차에 관한 입법례[64]

통신자료의 제공을 위해 사법적 판단을 요하는 국가는 미국, 독일 등이다. 미국의 경우 당사자가 동의하지 않는 이상 법원 및 대배심의 명령장이 필요하며 예외적으로 텔레마케팅 수사와 관련된 경우 수사기관의 문서로 제공이 가능하다. 반면 독일은 통신 미디어법 또는 전기통신사업법상

62) 이성기, 위 논문, 48면.
63) 이성기, 위 논문, 52면.
64) 이성기, 위 논문, 61면.

통신업체가 통신자료를 제공할 수 있도록 하는 근거규정은 있으나 통신업체가 이를 거부할 수도 있도록 재량사항으로 정하고 있다. 따라서 수사기관이 통신사업체가 협조하지 않는 경우 형사소송법에 의한 법원의 영장을 발부받아야 한다.

한편 영국은 국가안전보장, 범죄수사 및 예방, 공공의 안전 및 건강, 세금, 과태료 징수 등을 위한 목적 등 폭넓은 요건을 규정하면서 그 승인을 경찰 정보기관, 세관 등 각 기관들이 법령에 자체적으로 규정하도록 위임함으로써 비교적 폭넓게 통신자료의 제공이 가능하도록 규정하고 있다. 프랑스의 경우에는 사법기관은 통신자료를 요청할 수 있도록 하면서 경찰 및 군경찰 요원은 테러 및 국가안전을 목적으로 내무부 산하의 위원회의 결정을 거쳐 제공할 수 있도록 규정하고 있다. 한편 통신제공업자는 수사의 목적으로 최장 1년간 해당 자료를 보관할 수 있다.

일본은 수사기관이 우리나라와 같은 형사소송법상 사실조회 규정을 통하여 통신자료를 제공받을 수 있으나 이때에는 개별 통신과 직접적 관계가 없는 가입자의 인적사항, 주소 등 기본적인 사항만 제공이 가능하다. 기타 통신 상대방 등 통신과 직접 관련 있는 자료는 형사소송법상 영장이 있어야 한다.

3) 통신사실 확인자료 제공 요건과 절차에 관한 입법례[65]

우리나라와 달리 미국, 영국, 프랑스는 통신자료와 통신사실 확인자료의 구분 없이 제공 요건을 동일하게 규정하고 있다.

반면, 독일은 범죄수사와 관련하여 검사의 신청에 의해 법원의 명령을 받아 통신사실 확인자료를 제공받을 수 있으며 통신사실 확인자료의 범위는 통신내용 이외의 것으로서 우리나라의 것과 유사하게 규정되어 있다. 일본은 법원의 영장이 있거나 정당방위 또는 긴급피난 등 위법성 조각 사유가 있는 경우 통신사실 확인자료 제공을 받을 수 있다.

---

65) 이성기, 위 논문, 61면.

4) 소결

우리나라는 앞서 언급한 바와 같이 통신자료와 통신사실 확인자료를 구별하여 전기통신사업법과 통신비밀보호법에서 각 자료의 제공범위와 요건을 달리 규정하고 있다. 이중 통신사실 확인자료의 경우 통신비밀보호법 제13조 제1항과 제2항은 수사기관 등이 법원의 허가를 받아 전기통신사업자에게 통신사실 확인자료를 요청할 수 있도록 규정하고 있으며, 수사기관은 이 규정에 근거하여 법원의 허가를 사전 또는 사후적으로 받아 통신사실 확인자료를 취득하고 있으나, 법원의 심사가 일반 압수수색영장에 비해 형식적으로 이루어져 법원의 허가 없이도 제공되는 통신자료제공과 마찬가지로 남용되고 있다는 비판이 있다.

통신사실 확인자료는 당사자의 단순한 통신내역 뿐만 아니라 그 사람이 그 시각에 어디에 있었는지 현재 어디로 이동중인지 실시간 위치 정보를 파악할 수 있다는 점에서 통신의 자유 뿐만 아니라 신체의 자유도 침해할 수 있으므로 통신자료와 통신사실 확인자료를 구분하여 그 제공요건을 달리 규정한 우리 법제는 타당하다 하겠다.

다. 통신비밀보호법 상의 통신사실 확인자료 관련 규정

통신비밀보호법은 2001. 12. 29. 개정(법률 제6546호)을 통해 제3조 제1항에서 '누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실 확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다.'고 하여 종전의 우편물의 검열, 전기통신의 감청, 공개되지 않은 타인간의 대화 녹음, 청취만을 금지하던 것에서 '통신사실 확인자료의 제공' 금지를 추가하였다. 또한 2005. 1. 27. 개정(법률 제7371호)을 통해서는 제2조 제11호의 통신사실 확인자료의 정의 규정에서 종래 대통령령으로 규정되어 있던 컴퓨터 통신 또는 인터넷의 로그기록자료, 발신기지국의 위치추적자료, 정보통신기기의 접속지 추적자료 등을 새로이 포함시켰다.

따라서 크랙정보 수집프로그램을 통해 취득한 소프트웨어 불법복제 사용

자의 IP 주소가 '컴퓨터 통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기'의 위치를 확인할 수 있는 접속지의 추적자료'에 해당함은 당연한 것으로 보인다.

그런데 일각(특히 소프트웨어 불법복제 사용자를 고소한 저작권자의 입장)에서는 통신비밀보호법상의 통신사실 확인자료는 열거적 규정이므로 그 확장적 해석을 경계해야 할 것인데, 불법 복제 소프트웨어를 사용하는 자의 주된 목적은 인터넷 등 정보통신망의 접속이 아닌, 소프트웨어를 이용한 오프라인상의 작업이 주된 것으로 해당 사용자의 IP 주소 등의 정보는 소프트웨어 실행시 인터넷을 통해 기계적으로 전송된 접속지 IP 주소일 뿐이므로, 정보통신망에 접속할 목적과 무관한 정보통신기기의 위치여서 위 조항의 통신사실 확인자료에 해당하지 않는다고 주장하고 있다.

그러나 정보통신망 접속을 유일한 목적으로 컴퓨터 등 정보통신기기를 사용한 사람의 접속지 주소만이 통신사실 확인자료로 보호된다는 것은 사용자의 주관적인 목적에 따라 보호대상 해당 여부를 달리하는 것으로 법적 안정성을 해칠 뿐 아니라, 정보통신기구, 사물인터넷의 발달 등으로 일상생활의 대부분이 정보통신과 연계되어 사용되는 오늘날은 정보통신망 접속이 주된 목적인지 여부를 경계 짓기도 어려워 합리적이지도 않다.

따라서 크랙정보 수집프로그램을 통해 획득한 IP 주소 역시 '통신사실 확인자료'에 해당함은 부인할 수 없을 것이다.

그렇다면 통신비밀 보호법 제3조에서 '누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실 확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다'고 규정하고 있는 것과 관련해, 이 법률이 수사기관의 아닌 사인에게도 적용되는 것으로 저작권자가 수사기관에 고소하며 위와 같이 취득한 IP 주소를 제공하는 것 역시 금지되는 것이 아닌지가 문제된다.

라. 통신비밀보호법 제3조 규율대상

통신비밀보호법 제3조 외에도 제14조 역시 '누구든지 공개되지 아니한 타인간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취할 수 없다'고 규정하고 있다.

이때의 '누구든지'를 누구로 볼 것인지에 대하여는 제3조에 '통신사실 확인자료 제공 금지' 규정이 명문화되기 이전부터 수사기관을 포함한 국가기관과 일반 사인을 그 대상으로 한다는 견해[66], 수사기관을 포함한 국가기관만을 그 대상으로 한다는 견해[67] 등으로 나누어 학설의 대립이 있었다.

헌법에 의한 사생활의 자유 및 통신의 비밀은 기본권의 대사인적 효력에 따라 사인간에도 적용된다. 국가는 사생활의 비밀보장에 중요한 개인의 정보지배권을 보호할 의무가 있을 뿐만 아니라(헌법 제10조), 사인에 의한 통신의 비밀침해에 대하여는 형법상 비밀침해죄(형법 제316조)에 의하여 규율되고 있는 점 등에 비추어 볼 때 일반적으로 사생활의 비밀과 자유보장, 통신의 비밀보장은 국가뿐만 아니라 사인에게도 미치는 것[68]으로 이해함이 타당하다.

기본적으로 통신비밀보호법은 사생활의 자유와 통신의 비밀을 보호하는데 그 목적을 두고 있는 점, 그 규정 방식을 '누구든지'라고 규정하고 있을 뿐, 사인 또는 국가기관에 명백히 제한하여 규정하고 있지 않는 점 등에 비추어 볼 때 통신비밀보호법은 기본적으로 사인과 수사기관을 포함한 국가기관 모두에 대하여 적용된다[69]고 봐야 한다.

종래의 위와 같은 논의에도 불구하고 통신비밀보호법 제3조 중 특히 통신사실 확인자료 제공에 관하여는 다른 해석을 해야 한다는 견해도 있다. 그 근거로는 통신비밀보호법에서 통신사실 확인자료 제공에 관해서는 제3

---

66) 하태훈, "사인이 비밀리에 녹음한 녹음테이프의 증거능력," 「형사판례연구(8)」(2000), 514면; 이상돈,「사례연습 형사소송법」(2001), 356면.

67) 김대휘, "사진과 비디오테이프의 증거능력," 「형사판례연구(6)」(1998), 447면; 원형식, "형사소송법상의 증거사용금지에 관한 연구," 「형사정책연구」 제33호 (1998/봄), 231면; 안경옥, "형사절차상 사인이 녹음한 비디오테이프의 증거능력," 「사법행정」(1999/9), 15면.

68) 허영, 「헌법이론과 헌법」(2001), 398면.

69) 박미숙 "사인에 의한 비밀녹음테이프의 증거능력",「형사판례연구 11권」박영사 (2003. 6.)

조와 제13조에서 규정하고 있는데, 이중 제13조는 수사기관, 법원 등이 전기통신사업자에게 통신사실 확인자료 제공을 요청하는 절차 등을 규정한 것이므로 제3조는 위 절차를 위반하여 통신사실 확인자료를 제공하지 말라는 원칙을 확인한 금지규정 일 뿐이라는 것이다.

즉 통신비밀보호법 제3조 제1항에서는 ① 우편물의 검열금지, ② 전기통신의 감청 금지, ③ 통신사실 확인자료의 제공 금지, ④ 공개되지 아니한 타인간의 대화 녹음 또는 청취 금지 등 4가지를 규율하고 있는데, 통신비밀보호법은 위 ①, ②, ④의 행위와 이들 행위로 지득한 내용을 공개하거나 누설하는 행위를 처벌하는 벌칙규정[70]을 두고 있으나 ③의 통신사실 확인자료 제공금지 행위의 경우 처벌하는 규정을 두고 있지 않다는 것을 그 근거로 들고 있다.

즉 ①, ②, ④의 행위는 직접적으로 1차적인 행위를 금지하고 있는데 반해, ③은 1차적으로 취득한 자료를 2차적으로 외부에 제공하는 것을 금지하고 있고, ③의 구성요건을 충족시키기 위해서는 사전에 통신사실 확인자료를 취득 또는 수집하는 행위가 선행되어야 한다는 것이다. 그런데 통신비밀보호법은 제13조에서 수사기관, 법원 등이 적법하게 통신사실 확인자료를 제공받기 위한 절차를 규정하고 있을 뿐이다. 위 제13조에서 수사기관, 법원 등은 일정한 요건하에 '전기통신사업법에 의한 전기통신사업자

---

70) 제16조(벌칙) ① 다음 각호의 1에 해당하는 자는 1년 이상 10년 이하의 징역과 5년 이하의 자격정지에 처한다. <개정 2014.1.14.>
1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자
2. 제1호의 규정에 의하여 지득한 통신 또는 대화의 내용을 공개하거나 누설한 자
② 다음 각호의 1에 해당하는 자는 10년 이하의 징역에 처한다. <개정 2005.5.26.>
1. 제9조제2항의 규정에 위반하여 통신제한조치허가서 또는 긴급감청서등의 표지의 사본을 교부하지 아니하고 통신제한조치의 집행을 위탁하거나 집행에 관한 협조를 요청한 자 또는 통신제한조치허가서 또는 긴급감청서등의 표지의 사본을 교부받지 아니하고 위탁받은 통신제한조치를 집행하거나 통신제한조치의 집행에 관하여 협조한 자
2.제11조제1항(제14조제2항의 규정에 의하여 적용하는 경우 및 제13조의5의 규정에 의하여 준용되는 경우를 포함한다)의 규정에 위반한 자
③ 제11조제2항(제13조의5의 규정에 의하여 준용되는 경우를 포함한다)의 규정에 위반한 자는 7년 이하의 징역에 처한다. <개정 2005.5.26.>
④ 제11조제3항(제14조제2항의 규정에 의하여 적용하는 경우 및 제13조의5의 규정에 의하여 준용되는 경우를 포함한다)의 규정에 위반한 자는 5년 이하의 징역에 처한다.

에게’ 통신사실 확인자료의 열람이나 제출을 요청할 수 있도록 하고 있다. 통신비밀보호법은 통신 비밀과 자유를 보호하기 위한 법이고, 여기에서 통신은 우편물, 전화・전자우편・회원제정보서비스・모사전송・무선호출 등의 전기통신을 의미한다. 따라서 통신사실 확인자료는 전기통신역무를 제공하는 전기통신사업자[71]의 전기통신설비를 이용할 때 생성되는 정보 및 자료를 가리키는 것이므로 수사기관, 법원은 전기통신사업자에게만 통신사실 확인자료의 열람, 제출을 요청할 수 있고, 결국 통신비밀보호법 제3조 제1항 “누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하

71) 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2011.5.19., 2013.3.23., 2013.8.13., 2014.10.15.>
1. "전기통신"이란 유선·무선·광선 또는 그 밖의 전자적 방식으로 부호·문언·음향 또는 영상을 송신하거나 수신하는 것을 말한다.
2. "전기통신설비"란 전기통신을 하기 위한 기계·기구·선로 또는 그 밖에 전기통신에 필요한 설비를 말한다.
3. "전기통신회선설비"란 전기통신설비 중 전기통신을 행하기 위한 송신·수신 장소 간의 통신로 구성설비로서 전송설비·선로설비 및 이것과 일체로 설치되는 교환설비와 이들의 부속설비를 말한다.
4. "사업용전기통신설비"란 전기통신사업에 제공하기 위한 전기통신설비를 말한다.
5. "자가전기통신설비"란 사업용전기통신설비 외의 것으로서 특정인이 자신의 전기통신에 이용하기 위하여 설치한 전기통신설비를 말한다.
6. "전기통신역무"란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다.
7. "전기통신사업"이란 전기통신역무를 제공하는 사업을 말한다.
8. "전기통신사업자"란 이 법에 따른 허가를 받거나 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다.
9. "이용자"란 전기통신역무를 제공받기 위하여 전기통신사업자와 전기통신역무의 이용에 관한 계약을 체결한 자를 말한다.
10. "보편적 역무"란 모든 이용자가 언제 어디서나 적절한 요금으로 제공받을 수 있는 기본적인 전기통신역무를 말한다.
11. "기간통신역무"란 전화·인터넷접속 등과 같이 음성·데이터·영상 등을 그 내용이나 형태의 변경 없이 송신 또는 수신하게 하는 전기통신역무 및 음성·데이터·영상 등의 송신 또는 수신이 가능하도록 전기통신회선설비를 임대하는 전기통신역무를 말한다. 다만, 미래창조과학부장관이 정하여 고시하는 전기통신서비스(제6호의 전기통신역무의 세부적인 개별 서비스를 말한다. 이하 같다)는 제외한다.
12. "부가통신역무"란 기간통신역무 외의 전기통신역무를 말한다.
13. "특수한 유형의 부가통신역무"란 다음 각 목의 어느 하나에 해당하는 업무를 말한다.
가. 「저작권법」 제104조에 따른 특수한 유형의 온라인서비스제공자의 부가통신역무
나. 문자메시지 발송시스템을 전기통신사업자의 전기통신설비에 직접 또는 간접적으로 연결하여 문자메시지를 발송하는 부가통신역무
14. "전기통신번호"란 전기통신역무를 제공하거나 이용할 수 있도록 통신망, 전기통신서비스, 지역 또는 이용자 등을 구분하여 식별할 수 있는 번호를 말한다.

지 아니하고는 통신사실 확인자료의 제공을 하지 못한다"는 규정의 '누구든지'는 사실상 '전기통신사업자의 전기통신설비를 이용할 때 생성되는 (통신사실 확인)자료를 취득한 자'로서 '전기통신사업자'를 의미한다고 제한적으로 해석해야 한다는 것이다.

일견 설득력이 있는 주장이지만 규범체계상 제14조 보다 앞서 제3조에서 규정한 내용이 제14조의 규정을 전제로 그 원칙을 다시 선언 내지 확인하는 규정에 불과하다는 것은 체계적 법률해석에 어긋나고, 앞서 검토한 바와 같이 통신비밀보호법 제3조, 제14조의 '누구든지'는 문언의 의미 그대로 사인 모두를 포함하여 규율대상으로 본다는 것이 문언적 해석상 타당하며, 우편물의 검열, 전기통신의 감청 등의 경우와도 형평이 맞다고 할 것이어서 위와 같은 주장은 지나친 축소해석이라 할 것이다.

마. 통신비밀보호법 제3조를 위반해서 제공된 통신사실 확인자료의 증거능력

1) 통신비밀보호법과 위법수집증거배제법칙

통신비밀보호법은 불법검열에 의하여 취득한 우편물이나 그 내용 및 불법감청에 의하여 지득 또는 채록된 전기통신의 내용에 대하여 재판 또는 징계절차에서 증거로 사용할 수 없다고 규정하고 있으며(법 제4조), 이를 공개되지 아니한 타인간의 대화 및 통화내용을 녹음 또는 청취하는 경우에도 적용하도록 하여(법 제14조 제2항) 증거배제규정을 두고 있다. 이는 오늘날 사생활의 자유와 통신비밀에 대한 침해는 국가기관뿐만 아니라 사인에 의하여도 빈번하게 일어나고 있는 실정임을 감안하여 국가기관뿐만 아니라 사인에 의한 사생활 및 통신비밀 침해행위에 의하여 얻은 증거의 사용을 배제한 데 그 취지가 있다.

위와 같은 증거사용배제의 의미를 어떻게 파악할 것인가에 대하여, 구형사소송법에서 위법수집증거배제법칙을 명문화하기 전에는 위법하게 수집된 증거의 증거능력을 배제하는 미국법의 위법수집증거배제법칙을 인정한 것이라고 보는 입장[72]과, 위법수집증거배제법칙을 입법화한 것은 아니라

72) 변종필, "사인에 의한 위법수집증거와 그 증거능력," 「고시계」(2000/5), 93면; 이상돈, "혈액

고 하는 입장[73]으로 나뉘어 학설대립이 있었다. 그러나 2007. 6. 1. 형사소송법 제308조의2에서 '적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다'는 위법수집증거배제법칙을 명문으로 선언한 이후로는 위와 같은 학설대립은 크게 의미가 없고, 다만 위법수집증거배제법칙을 사인에 의해 수집된 증거에도 적용될 수 있을 것인지에 대한 문제가 남았다.

대부분의 학자들이 이를 인정하자는 데는 동의하고 있다. 즉 형사소추 및 실체적 진실발견이라는 공익과 개인의 사생활보호라는 사익을 비교형량하여 결정하여야 한다는 것이 일반적인 견해이다.[74] 긍정하는 견해 중에서도 크게 보아 기본권의 핵심적 영역이 침해된 경우에는 사인이 수집한 증거에 대하여 증거능력을 부정해야 하고 그 외의 영역에서는 이익교량에 의하여야 한다는 견해[75]도 있다. 한편 위법수집증거배제법칙은 수사기관에 한하여 인정될 뿐이고, 사인이 위법한 방법으로 증거를 수집하고, 수사기관이 위법행위를 권유하거나 위법행위에 관여하지 않은 경우에는 적용되지 않는다는 견해[76]도 있다.

대법원은 제3자가 공갈목적을 숨기고 피고인의 동의하에 나체사진을 찍은 경우, 그 사진을 피고인에 대한 간통죄의 증거로 사용할 수 있는지 여부[77]가 쟁점이 된 사안과 간통죄의 고소권자가 피고인이 그 주거에서 사실상 거주를 종료한 이후에 주거에 침입하여 혈흔이 묻은 휴지들 및 침대 시트를 수집한 사안[78]에서 이들 사인이 수집한 증거가 '적법한 절차에 따르지 아니하고 수집한 것으로 증거로 할 수 없는지'에 대하여 "모든 국민의 인간으로서의 존엄과 가치를 보장하는 것은 국가기관의 기본적인 의무

압수와 정보지배권," 「저스티스」 제34권

73) 신동운 "위법수집증거배제법칙과 나체사진의 증거능력," 「서울대법학」 제40권 제2호 (1999), 374면.

74) 조국, "위법수집증거배제법칙"(2005), 458면

75) 서보학, "위법수집증거의 쟁점 : 독수독과의 원칙과 예외, 사인이 위법수집한 증거의 증거능력", 「형사정책연구」제20권 제3호, 2009, 31면; 신양균, 「형사소송법」, 법문사, 2009, 744면; 이은모, 「형사소송법」(제3판), 박영사, 2012, 547면; 최영승, 「형사소송법」(제2판), 피앤씨미디어, 2013, 485면; 하태훈, 앞의 글(주 2), 523면.

76) 안성수, 「형사소송법」, 박영사, 2010, 321면.

77) 대법원 1997. 9. 30. 선고 97도1230 판결

78) 대법원 2010. 9. 9. 선고 2008도3990 판결

에 속하는 것이고, 이는 형사절차에서도 당연히 구현되어야 하는 것이기는 하나 그렇다고 하여 국민의 사생활 영역에 관계된 모든 증거의 제출이 곧바로 금지되는 것으로 볼 수는 없고, 법원으로서는 효과적인 형사소추 및 형사소송에서의 진실발견이라는 공익과 개인의 사생활의 보호이익을 비교형량하여 그 허용 여부를 결정하고, 적절한 증거조사의 방법을 선택함으로써 국민의 인간으로서의 존엄성에 대한 침해를 피할 수 있다고 보아야 할 것"이라는 이유로 위법수집증거로서 증거능력이 배제된다고 볼 수는 없다고 판시하고, 피고인이 시청 전자문서시스템을 이용해 보낸 전자우편을 시청 소속 공무원인 제3자가 권한없이 전자우편에 대한 비밀 보호조치를 해제하는 방법으로 수집한 전자우편에 대하여 "이 사건 전자우편을 수집한 행위는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조 제11호, 제49조 소정의 '정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀을 침해 또는 누설하는 행위'로서 형사처벌되는 범죄행위에 해당할 수 있을 뿐만 아니라, 이 사건 전자우편을 발송한 피고인의 사생활의 비밀 내지 통신의 자유 등의 기본권을 침해하는 행위에 해당한다는 점에서 일응 그 증거능력을 부인하여야 할 측면도 있어 보이나 이 사건 전자우편은 ○○시청의 업무상 필요에 의하여 설치된 전자관리시스템에 의하여 전송·보관되는 것으로서 그 공공적 성격을 완전히 배제할 수는 없다고 할 것이며, 또한 이 사건 형사소추의 대상이 된 행위는 구 공직선거법(2010. 1. 25. 법률 제9974호로 개정되기 전의 것)제255조 제3항, 제85조 제1항에 의하여 처벌되는 공무원의 지위를 이용한 선거운동행위로서 공무원의 정치적 중립의무를 정면으로 위반하고 이른바 관권선거를 조장할 우려가 있는 중대한 범죄에 해당하여 (중략) 이 사건 전자우편을 이 사건 공소사실에 대한 증거로 제출하는 것은 허용되어야 할 것이고,이로 말미암아 피고인의 사생활의 비밀이나 통신의 자유가 일정 정도 침해되는 결과를 초래한다 하더라도 이는 피고인이 수인하여야 할 기본권의 제한에 해당한다고 보아야 할 것이어서 원심이 이 사건 전자우편과 그 내용에 터잡아 수사기관이 참고인으로 소환하여 작성한 공소 외 2, 공소 외 3, 공소 외

4에 대한 각 진술조서들의 증거능력을 인정한 조치는 정당하다“고 판시하여 사인의 위법수집증거에 대해 비교형량을 통해 허용여부를 결정하고 있다.[79] 그러나 제3자가 피고인들 간의 전화통화를 녹음한 녹음테이프의 검증조서에 관하여 타인간의 대화를 녹음한 것으로 통신비밀보호법 제14조 제2항 및 제4조의 규정에 의하여 증거능력이 없다고 한 사안[80]에서와 같이 사인이 증거를 수집하는 과정이 직접적으로 법률의 금지규정을 위반하였거나 범죄에 해당하는 정도의 위법이 있는 경우에는 비교형량을 거치지 않고 곧바로 증거능력이 없다고 하는 것이 타당하다. 위에서 본 사안들의 경우에도 증거가 피촬영자의 동의 없이 찍힌 나체사진이거나, 타인이 거주하고 있는 주거지에 침입하여 증거를 수집한 경우였다면 각 성폭력범죄의처벌등에관한특례법위반(카메라등이용촬영)죄, 형법상의 주거침입죄 등에 해당할 것이고 그 경우, 위법성의 정도가 매우 중하고 직접적이므로 비교형량을 하여도 국민의 인간으로서의 존엄성에 대한 침해가 더 크므로 증거능력을 부정함이 마땅하다는 결과가 도출될 여지가 있다. 그렇게 되면 비교형량의 결과가 사실상 법관의 자의에 의해 달리 결정될 수 있어 법적 안정성을 해치게 된다는 점에서 부당하다. 따라서 사인이 수집한 위법수집 증거의 경우 그 사인이 증거를 수집하는 과정의 행위가 곧바로 법률을 위반하거나, 범죄를 구성하는 경우라면 별도의 비교형량 과정 없이도 형사소송법 제308조의2를 적용하여 증거능력을 배제할 필요가 있다.

미국에서 먼저 인정된 위법수집증거배제법칙은 일차적으로 수사기관의 적법절차 준수를 담보하는데 그 목적이 있었다. 그러나 근대적 형사소송관이 자리잡아가고 있는 오늘날에는 국가기관에 의한 기본권의 침해행위가 많이 줄어든 것이 사실이다. 대신에 사적 영역이나 사인에 의한 기본권의 침해행위가 빈번하게 발생하고 있으며 오히려 이를 통제하여야 할

79) 이에 대해 대법원 판례가 외견상으로는 이익형량설을 취한 것으로 보이지만 실제로는 사인의 기본권을 현저하게 침해한 경우라도 형식적인 교량을 통해 증거능력을 긍정해 버린 점에서 사인이 위법한 방법으로 증거를 수집한 경우에는 위법수집증거배제법칙이 적용되지 않는다는 입장을 취한 것이라고 보는 견해도 있다; 신양균,“우리나라 형사소송법상 위법수집증거배제법칙”, 「형사법연구」 제26권 제2호 (2014)

80) 대법원 2001. 10. 9. 선고 2001도3106 판결

필요성이 높아졌다.

또한 위법수집증거배제원칙을 인정하게 된 헌법적 근거 및 그 대사인적 효력 등을 고려하면 단순히 수사기관의 위법수사 억제라는 틀에서 벗어나 그 외연을 넓혀갈 필요성이 있다고 보인다[81].

2) 사인이 취득·제공한 통신사실 확인자료의 증거능력

앞서 보았듯이 통신비밀보호법 상에는 위법수집증거 배제규정에서 통신사실 확인자료가 누락되어 있다 하여도, 형사소송법의 개정으로 위법수집증거배제원칙의 일반규정이 신설되었고 그 사인적 효력도 인정하는 것이 타당하므로 제3조 금지규정을 위반하여 사인이 무단으로 수집, 제공한 통신사실 확인자료는 직접적으로 법률규정을 위반하여 위법한 증거로 비교형량을 통해 그 적법절차의 위반여부를 논할 영역을 벗어난 것으로서 형사소송에서 증거능력이 배제된다고 봄이 상당하다. 더구나 위 자료인 IP 주소 등을 제출하며 소프트웨어 불법복제 사범에 대한 저작권법 위반으로 고소하는 경우에는, 후속절차로 수사기관의 강제수사 특히 압수수색 등이 예상된다 할 것이어서, 단순히 사인이 수집한 불법한 증거의 문제에 그치지 않는다. 사인의 행위에 국가기관이 어떠한 형태로든 관여하였거나 관여할 것이 예정되어 있다면 상호관련성이 있다고 보아 이는 국가기관의 행위로 보거나 혹은 의제할 수 있기 때문[82]이다.

그럼에도 이와 달리 사인이 위법하게 취득하여 제공한 IP 주소 등의 통신사실 확인자료는 통신비밀보호법 제4조에서 위법수집증거로 명시적으로 설시하지 않고 있으므로 위법수집증거배제법칙이 적용되지 아니한다는 주장도 있다. 즉 통신비밀보호법 제4조는 “제3조의 규정에 위반하여, 불법검열에 의하여 취득한 우편물이나 그 내용 및 불법감청에 의하여 지득 또는 채록된 전기통신의 내용은 재판 또는 징계절차에서 증거로 사용할 수 없다.”는 내용으로 위법수집증거를 구체적으로 설시하고 있는 바, 위법수집

81) 최영승, 정영일, “사인이 위법하게 수집한 증거의 증거능력; 헌법적 근거에서, 그리고 주요 유형을 중심으로” 「경희법학」 제48권 제4호(2013) 14면.
82) 허영, 「헌법이론과 헌법」, 박영사, 2005, 390면

증거의 예로 ① 불법검열에 의하여 취득한 우편물이나 그 내용, ② 불법감청에 의하여 지득 또는 채록된 전기통신의 내용만을 들고 있으며, 같은 법 제14조 제2항은 제4조를 ④ 공개되지 아니한 타인간의 대화 녹음, 청취에 관해 준용하게 하였기에 결국 제3조의 규정에서 금지하고 있는 행위 중 ③ 통신사실 확인자료에 대하여만 위법수집증거로 사용을 금지하는 규정을 두지 않은 것은 이를 위법수집증거로 보지 않으려는 입법자의 결단이라는 주장이다.

이와 같은 주장은 특히 소프트웨어 불법복제 사용자를 고소한 저작권자나 그 고소대리인 측에서 선호하는 것으로 통상 고소인은 소프트웨어 제작사일 뿐 전기통신사업법상의 전기통신사업자가 아니므로, 크랙정보 수집프로그램을 통해 취득한 정보는 전기통신사업자가 전기통신역무를 제공하면서 발생한 것이 아니어서 통신비밀보호법 제3조, 제14조의 적용이 배제되고, 나아가 제4조에서 위법수집증거로 규정하고 있지 않으므로 형사소송의 증거로도 활용할 수 있다는 논리로 이어진다.

그러나 앞서 검토한 바와 같이 통신비밀보호법 제3조는 일반 사인을 포함한 모두를 규율대상으로 하여 금지하는 규정으로 봄이 상당하고, 형사소송법의 위법수집증거배제법칙의 대사인적 효력을 인정하는 이상 위와 같은 주장은 받아들이기 어렵다. 오히려 소프트웨어 저작권의 자산적 보호 필요성과 불법행위 처벌 및 근절 필요성만을 강조하며 해당 크랙정보를 수사의 단서로 활용하기 위해 법리적으로 무리한 주장을 펼치는 것은 적법절차의 원칙을 훼손하고, 자칫 절차상의 위법을 이유로 형사소송에서 증거로 쓰이지 못해 위법행위한 자에 대해 면죄부를 부여하게 될 위험이 있다. 이와 같은 주장을 관철하여 무리하게 강제수사를 진행하려는 시도 자체로 법치주의에 위협이 되는 것이다.

3) 통신비밀보호법 해석의 문제점과 입법론적 제안

그러나 저작권자의 권리구제 측면에서 저작권 침해를 입은 피해자로서의 저작권자가 수사기관에 처벌의사를 표명하기 위해 고소하며, 그 소명

자료로 활용하기 위해 저작권 침해행위를 한 자의 IP 주소를 제공하는 것을 당사자가 아닌 제3자로서의 통신사업자가 자신과 무관한 제3자의 범죄혐의에 대한 증거자료로 활용하기 위해 수사기관에 협조하는 경우와 달리 볼 필요성은 있다.

따라서 피해자로서 수사기관이 아닌 사인의 통신사실 확인자료의 수집 및 제공의 문제를 어떻게 볼 것인가의 문제는 해석론이 아닌 입법론적 차원에서 논의되어야 한다.

이를 법적 근거 없이 허용한다면 수사기관이 영장을 청구해야만 통신사실 확인자료를 구할 수 있는 것과 비교해 그 요건을 지나치게 완화하는 결과가 야기되어 불합리하고, 우리법이 자력구제라는 명목하의 불법행위를 허용하지 않고 있는 이념과도 모순되기 때문이다.

또한 통신비밀보호법은 위와 같은 3조의 금지규정을 두면서, 개인정보보호법과 달리 정보주체의 동의를 금지의 예외조건으로 두지 않았다. 이는 통신사실 확인자료에 정보주체의 처분권을 부정해야 할 정도로 고도의 보호 필요성을 인정한 것으로 보아야 할지 문제된다. 물론 통신의 경우, 본질적으로 상대방의 존재를 전제로 하고, 다수 당사자가 관여하므로, 개인정보에 비해 본인의 동의만으로 그 처분을 할 수 있다고 인정하기는 어렵다는 차이가 있을 수 있지만, 현행 법 해석상으로는 통신의 한 주체가 자신의 IP 주소를 공개하고, 타인에게 알려주는 경우 역시 위 법 제3조에 위배되는 것으로 보게 될 가능성이 있다.

위와 같은 통신비밀보호법 해석상의 모순과 허점에 대해 입법론적 해결방안이 필요하다.

Ⅴ. 소프트웨어 불법복제 방지를 위한 법제도 정비의 구체적인 제안

1. 사인인 저작권자의 사전적 증거수집 허용근거 규정 필요성

입법론적 해결 없이는 저작권의 직접 이용통제, 접근통제의 방법이 아닌,

형사고소를 통한 처벌을 전제로 하는 증거 수집 행위를 기술적 보호조치의 일환으로 인정할 근거도 미약하다. 이미 우리법은 기술적 보호조치의 유형을 정하고 있고 그 보호범위도 명확히 하고 있어, 무작정 이를 확장하는 것은 저작권의 공정 이용의 이념에 반하고, 저작권으로 보호하고자 하는 대상을 넘어서 필요 이상으로 그 보호수단까지를 보호하는 불합리한 점이 있다.

즉, 본래 기존의 저작권법에 의해 보호되는 범위가 아님에도 불구하고 기술적 보호조치의 법적 보호를 통해 새로운 권리를 창설하는 경우가 되는데 이 권리들은 저작물에 대한 저작권과는 개별적인 권리로서 보호하는 것이기 때문에, 법률에 규제하는 규정이 없거나 법률에 의해 허용되는 경우가 아니라면 규정을 위반한 자는 저작권 침해 여부와는 별도의 법적 책임을 지게 된다.

DRM 기술 중 저작물에 대한 접근통제에 관한 기술은 기본적으로 저작물 제공자의 개인정보 수집과 이를 이용한 저작물에 대한 접근의 통제를 전제로 하고 있으며, DRM 기술에 포함된 감시기능은 소비자의 지적 소비활동을 낱낱이 감시・체크하고 지적 소비활동에 관한 정보의 수집・이용을 가능케 함으로써 소비자의 정보 프라이버시(information privacy)를 침해하는 문제[83]가 있다.

따라서 저작권자의 저작권 보호의 필요성과 저작권의 공정 이용, 저작물 사용자의 정보 프라이버시권 보호라는 대비되는 이익을 형량하여 조화롭게, 비례성 원칙에 부합하는 범위에서 사인의 사전적 증거수집행위를 허용하는 근거 규정을 구비할 필요성이 있다.

독일은 소프트웨어 불법복제의 단속에 민간인이 참여할 수 있게 하며, 그 근거로서 기본법(Grundgesetz)상의 국민의 의무를 제시하고 있다. 다만 형사절차에서 증거확보의 목적으로 제3자가 참여하는 것은 수사기관이 중요한 증거를 수집함에 있어서 특히 기술적으로 어려움이 있는 경우에

83) 이창범, “프라이버시 보호를 위한 DRM기술 리엔지니어링”, LAW & TECHNOLOGY, 제1권 제1호(창간호), 서울대학교 기술과법센터, 2005.7, 40면; 강기봉 “DRM기술을 둘러싼 개인정보 및 프라이버시의 법정책적 검토”, 「법과 정책연구」16권 2호, 한국법정책학회, (2016), 376면.

한하여 인정되며[84], 이 경우 그러한 참여로 인해 침해될 개인의 기본권을 고려하여 비례성 원칙에 따라 민간인이 참여하게 되는 수사의 내용, 목적 정도를 고려하여 그 허용여부를 결정해야 한다고 한다.[85]

통신비밀보호법 상의 허용되지 않는 통신사실 확인자료 수집·제공의 범위를 명확히 하고, 다만 통신주체의 동의 없이도 저작권자의 저작재산권 등 권리수호를 위해 필요한 경우 사인이 저작권 침해 행위자의 IP 주소 등 통신사실 확인자료를 수집·제공할 수 있는 근거규정을 입법화 하며 위와 같은 법익 형량을 고려해야 할 것이다.

2. 기술적 보호조치의 보호 정도에 따른 증거수집 허용의 차등화

가. 오픈소스 소프트웨어의 저작권 문제 대두

오픈소스 소프트웨어란, 소스코드를 제공하고 자유로운 배포가 가능한 소프트웨어를 말하며, 소프트웨어의 자유로운 사용, 수정, 재배포는 허용하나 이를 무조건 무료나 공짜로 사용할 수 있다는 것은 아니다. 저작권이 없는 퍼블릭 도메인 소프트웨어와는 구별되며, 오픈소스 역시 저작권을 가진다.[86]

오픈소스 소프트웨어는 상용 독점 소프트웨어와 달리 금전적인 대가 없이 프로그램을 사용할 수 있게 배포하기 때문에 대부분의 사용자는 무료인것처럼 느낄 수 있다. 하지만 오픈소스 소프트웨어가 무료라고 해서 아무런 대가 없이 사용하는 것은 아니며 세부적인 라이선스[87]의 요구사항을 준수하여야 합법적으로 이용할 수 있다.

이처럼 오픈소스라면 별도의 기술적 보호조치를 가지고 있지 않은 것이

84) 김상겸, "게임소프트웨어 불법복제에 관한 법적연구" (2014), 45면.
85) Wolfgang Bar, Beschlagnahme von Computerdaten, CR 1996.11.: 김상겸, 위 논문, 47면.
86) 한국저작권 위원회, 라이선스 소개 https://www.olis.or.kr/ossw/license/introduction.do (2016. 10. 23. 최종확인)
87) 오픈소스의 라이선스에 따라 지켜야 하는 의무도 다른데, 오픈소스를 수정했을 때는 소스배포의 의무를 가지며, 하나의 서비스라 할지라도 오픈소스와 별개의 모듈이라면 해당 모듈은 공개의 의무를 갖지 않거나, 사용에 대한 명시만 해줘도 되는 경우도 일반적이다.

일반적이고, 이 경우 저작권자가 사용자의 IP 주소 등 통신사실 확인자료를 수집, 제공한다면 설사 그 라이선스에 대한 침해가 있었다 할지라도 보호가치 있는 저작권보다 더 큰 침해를 야기하는 것으로 허용될 수 없다고 봐야 할 것이다. 이러한 침해를 이유로 저작권자가 사적으로 취득한 IP 주소 등을 제공하며 고소한다 해도, 이는 위법한 증거수집으로 이를 소명자료로 해서 압수수색영장 청구로 나아갈 수 없다고 보아야 한다.

최근 오픈소스 저작권과 관련한 분쟁이 늘어나고 있는데, 오픈소스 소프트웨어 라이선스에서 요구하는 준수사항을 이행하지 않아 권리자로부터 저작권 위반으로 소송을 제기당해 손해배상을 포함한 책임을 부담하거나, 형사 고소의 합의를 조건으로 막대한 합의금을 지급하는 경우도 늘고 있다. 최근에는 '폰트 저작권'과 관련, 일부 폰트 개발업체들이 폰트 파일을 무료로 사용할 수 있도록 인터넷에 풀었다가 어느 순간 유료로 전환하고, 유료화된 사실을 모르고 전에 컴퓨터에 저장해둔 파일을 사용한 사용자들을 상대로 저작권 위반으로 문제삼는 경우가 종종 있어 이슈가 되기도 했다.[88]

일반인의 법감정상으로는 기술적 보호조치를 취하지 않은 소프트웨어의 저작권을 철저하게 보호하는 과정에서 단지 무지하였거나 부주의했던 범법자를 양산하는 것에 대해 거부감을 갖게 되므로, 저작권자의 사전적 증거수집 허용근거 규정이 위와 같이 저작권 침해를 가장한 손해배상 및 형사 합의금 갈취(요구)의 수단으로 악용되지 않도록 기술적 보호조치의 보호 정도에 따라 증거수집 허용 여부를 달리 해야 할 것이다.

나. 기술적 보호조치의 보호정도 규격화와 차등 보호

위와 같은 오픈소스 소프트웨어가 아니라도, 유료 소프트웨어의 경우에도 스스로 무단 편집·불법 복제 방지를 위한 아무런 기술적 보호조치를 취하지 아니한 때에는 그 저작권 침해행위를 예상하고, 증거수집을 위해 사전적으로 사용자의 IP 주소 등 통신사실 확인자료를 수집하는 것을 허

88) 월간 midas 2016년 5월호 115면, 유진희 기자, '폰트 저작권이라고 들어보셨나요'

용할 필요성이 적다 할 것이다.

기술적 보호조치는 그 보호의 정도에 따라,

- 1단계 : 오픈소스 소프트웨어 및 유료 소프트웨어로서 별도의 기술적 보호조치 없이, 무단 편집, 불법 복제 등을 금지하는 내용의 경고 문구만을 포함하는 경우
- 2단계 : 시간제한을 두거나, 프로그램을 수행할 때마다 구매를 유도하거나 홍보하는 다이얼 로그 박스를 화면에 몇초간 출력하는 등의 프로텍션 기술을 사용하는 내그 스크린 프로그램을 사용하는 등으로 불법 사용 자체를 불가능하게 하지는 않지만 사용상 불편을 야기하는 정도의 보호조치를 취한 경우
- 3단계 : 소프트웨어 사용 자격을 정식 인증받기 위해 등록번호를 입력하게 하는 방식으로 암호화 기술을 사용하거나 사용자 인증을 받게 하는 등으로 불법사용자의 접근을 통제하는 적극적인 형태의 기술적 보호조치를 취한 경우
- 4단계 : 소프트웨어의 불법적인 복사를 방지하기 위해 컴퓨터의 I/O 포트에 작은 하드웨어를 부속시키는 동글(Dongle)을 이용하는 등으로 하드웨어를 접목시켜 소프트웨어를 보호하는 경우

와 같이 단계별로 구분할 수 있다. 이는 소프트웨어 무단 편집, 불법 복제를 위해서 사용자가 어느 정도의 적극적인 침해의사와 목적을 가지고, 저작물에 접근하는 것 이상의 침해행위가 개입되어야 하느냐에 따른 구분이다.

지속적으로 발전하고 진화하는 기술의 특성상 위와 같은 4단계의 구분 및 그에 포섭되는 구체적인 기술의 예시조차도 한시적일 수 있어, 보호조치의 정도와 그에 따라 예상되는 침해의 정도는 법률차원에서 규율[89]하되, 구체적인 기술적 보호조치의 차등기준 및 구체적인 예시규정은 시행

89) 구체적으로는 통신비밀보호법 제3조의 금지규정에 대한 예외규정으로 '통신사실 확인자료의 제공'을 허용하는 사유를 열거하는 형식을 취하며, 규범조화적인 체계를 위해서는 동법 제13조 '범죄수사를 위한 통신사실 확인자료제공의 절차'와 관련해 '소프트웨어 저작권자의 통신사실 확인자료 수집·제공'이라는 표제하에 저작권자가 소프트웨어 불법 복제 사용자의 통신사실 확인자료를 수집할 수 있다는 근거규정과 그 수집범위 및 범죄의 증거로 수사기관에 제공하는 구제적인 절차 및 요건을 규정하는 방식을 취해야 할 것이다.

령 차원에서 규율하여 잦은 개정으로 인한 법적안정성이 손상될 우려를 미연에 방지할 필요가 있다.

위와 같은 4단계의 보호조치 가운데 소프트웨어 무단 편집, 불법 복제 등을 위해서 프로그램의 조작, 위조, 새로운 프로그램의 생성, 활용 등의 적극적인 침해행위가 필요한 경우, 즉 3, 4단계 이상의 경우에만 저작권자로 하여금 그 불법 사용자의 IP 주소 등의 증거 수집을 허용하고 이를 수사기관에 제공할 수 있도록 하는 근거 조문을 구비하는 것이 합리적이고도 법익균형에 맞는 입법 방안일 것이다.

즉 저작권자가 소프트웨어에 대한 저작권으로 보호받고자 하는 의사를 표명하였으나, 별다른 보호조치를 취한 바는 없거나 단순한 경고에 그치는 경우와 소프트웨어 불법 복제 사용시에는 불편함을 느끼거나, 일부 부수적인 기능의 사용이 제한되는 정도의 보호조치만을 취한 경우에는 사용자는 별다른 침해행위 없이도 쉽게 소프트웨어를 무단 편집하거나 복제할 수 있게 된다. 즉 위법성의 인식이 미약한 채로도 충분히 위법행위를 하고 저작권 침해의 결과발생이 가능하다. 이는 소프트웨어 불법 사용을 용인하는 것에서 나아가 유인하는 환경이 될 수 있고, 고의 없이 결과를 야기한 경우까지를 사용자의 불법행위로 예정하고 저작권법 침해 사범으로 의율하며 형사처벌의 증거수집을 사전에 허용하는 것은 과잉형법이라는 비난을 피할 수 없다. 그 보호의 필요성 측면에서도 이러한 경우 저자권자의 안일한 태도는 스스로 권리를 수호하기 위해 노력하지 않았다는 점에서 이른바 '권리 위에 잠자는 자'라고 할 것이고, 사전적인 예방조치는 소홀히 하면서도 사후적인 침해의 경우는 강경히 대응할 것을 전제로 크랙정보 수집 프로그램을 활용한 증거수집을 하고자 하는 것은 자기모순적인 태도라는 점에서 그 필요성이 비교적 작다. 그럼에도 그 보호를 위해 불필요하게 다수의 국민을 잠재적인 범죄자로 취급하게 되는 점에서 불합리하다. 소프트웨어 저작권을 보호라는 법익과 사용자의 정보의 자유와 통신의 자유 등 기본권 침해의 측면을 비교형량 했을 때 비례의 원칙을 위반하는 것이다.

또한 1, 2단계의 위반의 경우는 저작권자가 허용한 소프트웨어 이용권한의 범위를 초과한 침해의 결과(오픈소스를 수정·가공하여 탄생한 2차 저작물을 유상 제공하는 경우 등)라는 것은 이미 대외적으로 불특정 다수의 사람들에게 드러나게 됨으로 이를 저작권 위반으로 처벌하기 위한 증거수집이 비교적 용이하므로, 사인에 의해 크랙정보 수집 프로그램을 활용한 사전 증거수집까지 허용할 필요성이 더욱 적다.

그러나 3, 4단계 이상의 기술적 보호조치를 취한 경우라면 저작권자로서도 강한 저작권적 보호를 받을 것임을 명백히 선언한 것이고 이 때의 기술적 보호조치는 침해의 목적, 적어도 고의 없이는 무력화하기 어려운 것이다. 따라서 저작권 침해자는 비난가능성이 더욱 높고, 스스로도 저작권법 위반으로 인한 형사처벌의 가능성을 인지하고 있는 경우가 많다. 또한 그와 같은 기술적 보호조치를 무력화한 경우라면 이를 외부에 유출, 판매하지 않아도 불법 복제하여 개인적으로 이용하는 것만으로도 이미 저작권 침해의 결과가 발생한 것이라고 할 것이어서 침해의 결과 발생 이후에도 증거수집이 어렵고, 복제 또는 수정한 프로그램을 간단히 삭제 또는 변형하는 방법으로 증거를 은닉하기도 손쉽다. 따라서 저작권자로 하여금 사전에 크랙정보 수집 프로그램을 활용해 불법 사용자의 크랙정보를 수집할 수 있는 근거 규정을 두고 그 가능성을 열어둘 필요성이 높다.

다. 소프트웨어의 가치와 기술적 보호조치의 보호정도

이때 기술적 보호조치의 정도가 그 보호대상인 소프트웨어의 프로그램으로서의 가치의 실질에 부합해야하는지 여부가 또 하나의 쟁점이 될 수 있다. 다시 말해 기존에 무료로 공개된 오픈소스 소프트웨어의 기능 이상을 가지고 있지 않음에도 과도한 기술적 보호조치를 접목해 보호하고 있는 소프트웨어의 경우, 기술적 보호조치의 침해 정도가 중대하다는 이유로 크랙정보 수집 프로그램을 이용한 크랙정보 수집을 사전에 허용하는 것이 정당한가의 문제이다.

하지만 해당 소프트웨어의 기술적 가치 및 그 침해로 인한 경제적 손해

의 산정은 민사상 배상의 영역에서 판단해야 할 것이고, 그 소프트웨어의 내용과 기능에 상관없이 기술적 보호조치의 정도 및 그 침해 유형에 따라 일괄적인 형사처벌 및 증거수집 가능성을 예정하는 것이 법적안정성 및 형사처벌의 정책적 취지에도 부합한다 하겠다. 즉 형법이 거주자의 주거의 평온을 보호하고자 주거침입을 처벌하면서, 그 거주자의 주거의 평온을 가치매겨 보호하거나 타인의 재물을 절취하는 절도죄를 처벌하면서 그 재물이 객관적인 교환가치를 가질 것을 요구하지 않는 것[90]과 같은 관점에서 생각할 수 있다.

위에서 구분한 바에 의하면, 3, 4단계 이상의 기술적 보호조치를 취한 경우, 이를 무력화하는 행위는 그 자체로 법익 침해의 고의를 드러낸 것이고 위법성이 충분히 실현되었기에 처벌의 대상이 되는 행위라 할 것이고, 이때의 소프트웨어의 내용 및 기능의 실질이 보호가치가 적다해도 이를 이유로 크랙정보 수집 프로그램을 활용한 저작권자의 증거수집이 부당하다고 판단하기는 어렵다. 더구나 위와 같은 구분에 따라 허용하는 것은 형사소송에서 증거로 활용하기 위한 크랙정보의 수집일 뿐 그 자체로 형사처벌의 수위를 달리하는 것은 아니기 때문에 이로 인해 정의에 반하는 결과가 야기된다고 예상하기는 어렵고 소프트웨어 실질적인 가치는 형사절차의 최종단계에서 양형사유로 참작하면 충분할 것이다.

현실적으로도 위와 같이 소프트웨어의 실질적인 가치를 이유로 저작권자가 취한 기술적 보호조치의 정도가 적정한 것인지 혹은 과도한 것인지를 사전에 결정해서 허용여부를 달리하기 위해서는 정부 또는 저작권협회 등 공신력 있는 제3의 기관에서 사전에 이를 판단 받을 수 밖에 없다는 문제가 있는데 이는 헌법상 표현의 자유와 관련, 언론 출판에 대한 사전 심의 내지는 검열을 금지하고 있는 취지를 고려할 때 부적절한 것으로 보인다.

---

90) 절도죄의 객체인 타인의 재물은 재산권 특히 소유권의 객체로 될 수 있는 물건임으로써 족하고 반드시 객관적인 금전적 교환가치를 가질 필요는 없다고 하며, 부모의 사진이나 애인의 편지 등과 같은 것은 객관적 교환가치는 없을지라도 그 소유자나 점유자에게 주관적인 감정가치가 있으므로 재물로서 형법적 보호의 대상이 된다고 하고 있음 - 주석형법 형법각칙, 한국사법행정학회, 2006. 4.(제4판) 제292쪽, 박재윤, 김경선

Ⅵ. 결론

오늘날 소프트웨어의 저작권은 보호해야할 개인의 사적 재산권 중 그 규모나 영향력 면에서 가장 중요한 것중 하나임에 틀림없다. 이러한 소프트웨어 불법 복제 방지는 사적 차원의 재산권 수호의 문제가 아닌 국가적 차원의 정책적 목표가 되었고, 피해를 입은 저작권자가 민형사상 방법으로 그 권리구제 방안을 모색하는 것은 비난받을 일이 아니다. 다만 소프트웨어 불법 복제 방지라는 목표를 수사기관에 대한 고소 및 그 후속조치로서의 압수수색등 강제수사로 이어지는 채증과정을 통한 협상의 우위확보, 구매계약 체결 강권, 합의 또는 계약 체결 후 고소취하라는 일련의 과정을 통해 달성하고자 하는 것은 국가 수사력의 낭비일 뿐 아니라, 기술진보의 측면에서도 바람직하지 않다.

따라서 지나치게 침해 이후의 사후적 구제조치, 그중에서도 증거 획득을 위한 모니터링, 정보 수집 등에 치우진 관심과 에너지를 소프트웨어 불법복제 방지를 위한 보안기술 개발 쪽으로 돌려, 사전적 예방 위주의 보호정책을 펼칠 필요가 있다. 이러한 사전적 예방으로서 기술적 보호조치를 충실히 한 소프트웨어에 대하여는 그렇지 않고 단순한 경고 문구 등으로 불법복제 금지를 선언하는 것에 그쳐, 불법복제를 용이하게 방조하는 소프트웨어와 달리, 그 저작권 침해자에 대한 통신사실 확인자료 등의 수집마저도 용인함으로써 사인의 저작권 보호를 보충하는 방향으로 법제도가 정비되어야 할 것이다.

[참고문헌]

강기봉, “DRM기술을 둘러싼 개인정보 및 프라이버시의 법정책적 검토”, 「법과 정책연구」 제16권 제2호, 한국법정책학회(2016. 6.)

장성민, 박정흠, 박한웅, 이상진, “Full Disk Encrytion 환경에서 디지털증거 수집절차에 관한 연구” 「정보보호학회 논문지」Vol. 25, No. 1, (2015. 2.)

박정현, “GPRS망을 방문한 이동 ISP 가입자의 무선인터넷 서비스를 위한 동적 IP 할당 방법”, 「정보처리학회논문지D」제11-D권 제4호(2004. 8.)

정연수, “IP주소와 MAC주소를 이용한 이블 트윈 탐지 기법”, 아주대학교 공학석사 학위논문(2012. 11.)

김홍일, 신판섭, “ISP별 IP 분포를 고려한 비구조적 Peer to Peer에서의 Look up 기법”, 「한국컴퓨터산업교육학회 논문지」, 2003. 12. , Vol 4.

“SW 역분석과 기술적 보호조치(법적・기술적 재해석)”, 「한국저작권위원회」(2009)

이충열, “클릭랩 약정의 효력 요건에 관한 연구-미국의 입법과 판례를 중심으로”, 「국제상학」제20권제3호(2005. 9.)

한국저작권위원회, 「SW역분석과 기술적 보호조치-법적, 기술적 재해석」(2009. 12. 4.)

이대희, “개인정보 개념의 해석 및 범위에 관한 연구”, 「고려법학」제79호, 고려대학교 법학연구원(2015. 12.)

신영진, “개인정보보호를 위한 기술적 보호호조치의 개선에 관한 연구”, 「공공정책과 국정관리」 제8권 제1호,(2014. 6.)

김재윤, “검사의 독점적 영장청구권과 통신사실 확인자료 요청허가청구권”, 「비교형사법연구」 제16권 제2호(2013)

김상겸, “게임소프트웨어 불법복제에 관한 법적연구”, 동국대학교 법학석사 학위논문 (2014. 6.)

허준, 홍충선, 이호재, “경량화된 IP 역추적 메카니즘”, 「정보처리학회 논문지C」 제14-C권 제1호(2007.2.)

정진명, “디지털 정보거래의 계약법적 규율과 그 한계”, 「法學論叢」, 제32권 제1호, 단국대학교 법학연구소(2008. 6.)

박종권, “디지털 콘텐츠 이용계약의 법적 성질과 권리・의무에 관한 고찰”, 「이화여자대학교 법학논집」 제14권 제1호, 이화여자대학교(2009. 9.)

愛甲健二, “리버스 엔지니어링 입문, 즐거운 리버싱”, 비제이퍼블릭(2014. 10.)

김현숙, “멀티유저 PC를 중심으로 살펴본 소프트웨어 이용허락계약 체결과 저작권 침해 문제”, 「안암법학」 Vol. 43 (2014. 1)

권양섭, “범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안”, 「법학연구」 제59집, 한국법학회 (2015)

하태훈, “사인이 비밀리에 녹음한 녹음테이프의 증거능력”, 「형사판례연

구(8)」(2000)

고병완, 송희석, “불법복제에 대한 규제가 콘텐츠제작자의 수익에 미치는 영향”, 「한국콘텐츠학회논문지」‘10 Vol. 10 No.2 (2010. 1.)

김대휘, “사진과 비디오테이프의 증거능력”, 「형사판례연구(6)」, 박영사(1998)

최영승, 정영일, “사인이 위법하게 수집한 증거의 증거능력”, 「경희법학」 제48권 제4호(2013)

박미숙, “사인에 의한 비밀녹음테이프의 증거능력”, 「형사판례연구 11권」, 박영사(2003. 6.)

류지영, “사인에 의한 위법수증거의 배제범위”, 「중앙법학」 제12집 제4호, 중앙법학회(2010. 12.)

차병래, “소프트웨어 자산관리를 위한 패키지 소프트웨어 점검서비스 구현”, 「한국콘텐츠학회논문지」Vol.7 No.1(2007)

최광준, “소프트웨어 계약과 라이선스 약관의 유효성”, 「경희법학」제44권 제1호, 경희대학교 (2009.6.)

오명신, 한승조, “소프트웨어 불법복제 방지를 위한 보안칩”, 「정보보호학회논문지」 제12권 제4호 (2002. 8.)

정완 “소프트웨어 불법복제 실태와 법제도적 개선방안”, 한국형사정책연구원 (2003. 12.)

김광용, “소프트웨어 불법복제에 따른 경제적 효과분석 및 정책방향 제시”, 「프로그램심의조정위원회 연구보고서」(2002. 4.)

한지영, “소프트웨어 불법행위와 인터넷에서 저작권 침해행위에 대한 법적보호”, 「법학교수 ·검찰 실무 연구회 발표자료집」, 광주지검 (2009)

차병래, “소프트웨어 소스코드의 저작권 관리를 위한 디지털 라이선스의 검색”, 「한국콘텐츠학회논문지」Vol.7 No.1(2007)

이정윤, “소프트웨어의 저작권법 문제와 극복방안 연구”, 인천대학교 정보기술대학원 석사학위논문 (2015. 12.)

전정화, “소프트웨어의 지적재산법적 보호방안에 관한 연구”, 광운대학교 법학 석사학위 논문 (2011. 7.)

차태원, 안재경, ″소프트웨어 자산관리를 위한 패키지소프트웨어 점검서비스 구현″, 「정보처리학회논문지D」 제16-D권 제1호 (2009. 2)

유진룡, 「엔터테인먼트 산업의 이해」, 넥서스 비즈, (2009)

차태원, 안재경, “온라인상의 콘텐츠 공유에 따른 소프트웨어 자작권 침해 실태 및 경제적 손실액 추정에 관한 연구”, 「정보통신정책연구」 제14권 제4호(2007. 12.)

신양균, “우리나라 형사소송법상 위법수집증거배제법칙”, 「형사법연구」 제26권 제2호, 한국형사법학회(2014)

박영규, “위조 및 불법복제 방지협정(ACTA)의 탄생, 의미 및 전망”, 「경영법률」21권 3호, 한국경영법률학회(2011)

김욱준, “위조 및 불법복제 방지협정(ACTA) 타결, 국제적 수준에서 온라인 저작권 집행노력 강화”,「정보통신방송정책」22권 19호(2010)

김요식, 윤영태, 박상서, “윈도우환경에서의 메모리 해킹방지 시스템 연구” 가야 ,「정보보증논문지」제5권 제3호(2005. 9.)

김병일, “인터넷 상의 저작물 불법유통에 대한 규제방안”, 「法學論叢」제33권 제2호, 단국대 법학연구소(2009. 12.)

탁희성, “저작권보호를 위한 기술적 보호조치에 관한 소고”, 「형사정책연구」제20권 제1호(2009)

이규홍, “저작권법상 기술적 보호조치의 법적 보호에 관한 연구-기술적 보호조치를 중심으로”, 「연세 의료·과학기술과 법」제1권 제1호, (2010. 2.)

박찬걸, 강동욱, “전기통신사업법상 통신자료제공제도의 문제점과 개선방안”, 「법과 정책연구」제14권 제1호, 한국법정책학회(2014. 3.)

박재윤, 김경선, 「주석형법 형법각칙」제4판, 한국사법행정학회(2006. 4.)

홍민지, “첨단기술의 유출방지를 위한 관련법규의 형사법적 문제점과 개선방안”, 인하대학교 법학 석사학위 논문(2007. 8.)

이충열, “클릭랩 약정의 효력요건에 관한 연구-미국의 입법과 판례를 중심

으로-",「국제상학」 제20권 제3호

이성기, "통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본의 제도 비교를 중심으로",「법과 정책연구」 제14권 제1호, 한국법정책학회 (2014. 3.)

김영태, "특수한 유형의 온라인서비스 제공자 책임제도의 개선방안-기술적 조치와 시정명령, 시정권고 제도를 중심으로", 「法學論叢」제40권 제1호 단국대학교 법학연구소(2016. 3.)

강호갑, "표준기술동향: DRM(Digital Rights Management)", TTA Journal, 제103호(2006)

이창범, "프라이버시 보호를 위한 DRM기술 리엔지니어링", LAW & TECHNOLOGY, 제1권 제1호(창간호), 서울대학교 기술과법센터(2005. 7)

최필주, 최원섭, 김동규, "하드웨어 칩 기반 보안시스템 및 해킹동향", 「한국통신학회지(정보와 통신)」, 한국통신학회(2014. 4.)

허영, 「헌법이론과 헌법」(2001)

Abstract

As reverse engineering technology advances, the threat of illegal manipulation and tampering with computer software is increasing.

And anybody can crack the software by using the simple tools on the internet. The software companies are struggling to defend their own softwares against the Crackers. As part of such efforts, they tend to use the Crack Information Gathering Program.

If a copyright owner has identified a suspect based on IP address collected through the use of a Crack Information Gathering Program, It can be regarded as a legitimate evidence for a search warrant?

It may be not allowed under the interpretation of the Communications Confidentiality Protection Act. If so, it is necessary to legislate related regulations for protecting of copyright and technical protection measure. We should permit copyright owner despite being a private person, to collect the Crack information and submit as evidence of software copyright infringement.

Especially, depending on the degree of technical protection measure, we can Provide differentiated legal protection in the scope and qualification of evidence collection.

Keyword: Crack Information Gathering Program, technical protection measure, software copyright infringement.

Student Number: 2016-26061